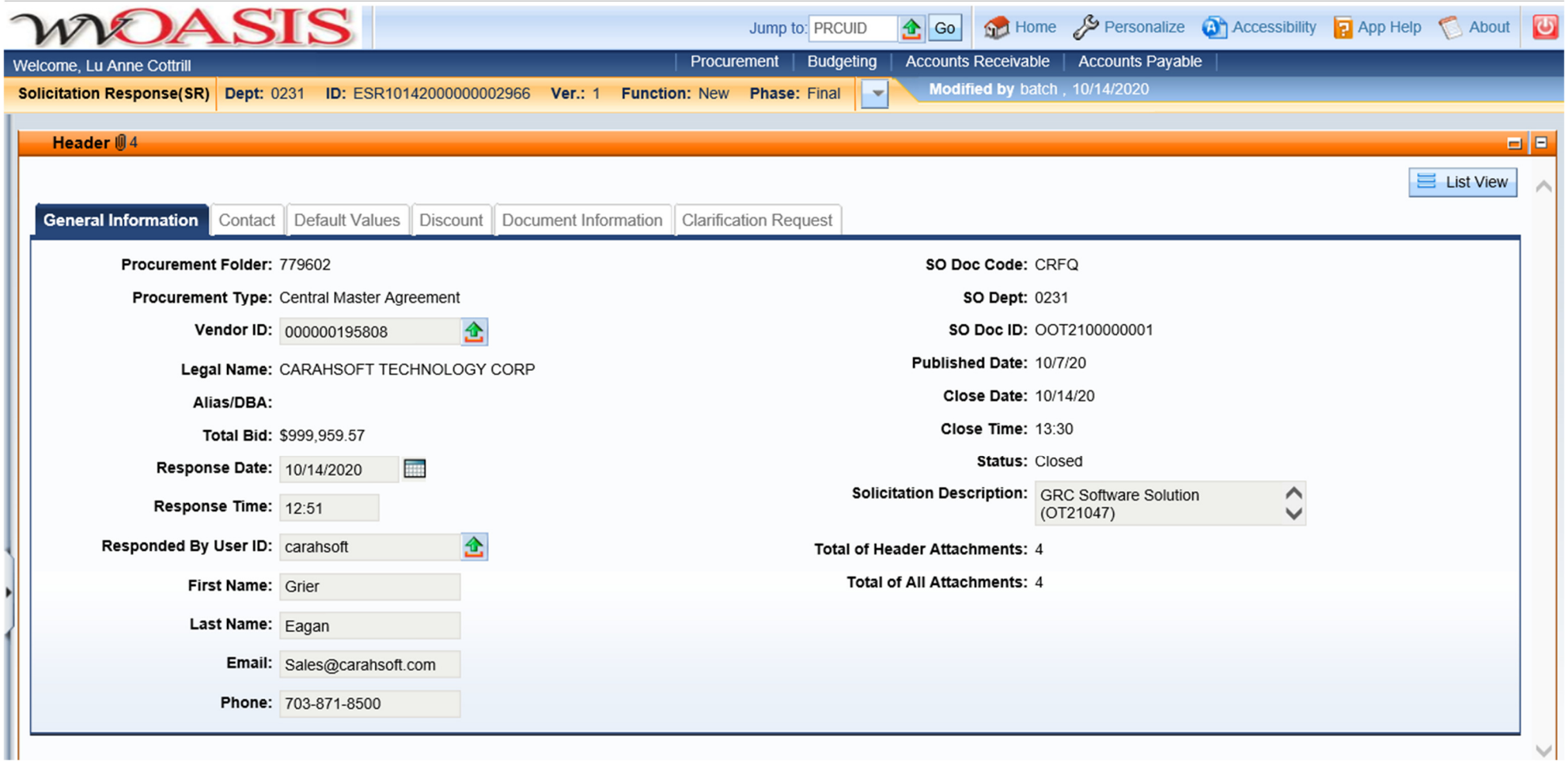
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: PRCUID Go
Home
Personalize
Accessibility
App Help
About
Welcome, Lu Anne Cottrill
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0231 ID: ESR10142000000002966 Ver.: 1 Function: New Phase: Final
Modified by batch , 10/14/2020
Header 4
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 779602
Procurement Type: Central Master Agreement
Vendor ID: 000000195808
Legal Name: CARAHSOFT TECHNOLOGY CORP
Alias/DBA:
Total Bid: $999,959.57
Response Date: 10/14/2020
Response Time: 12:51
Responded By User ID: carahsoft
First Name: Grier
Last Name: Eagan
Email: Sales@carahsoft.com
Phone: 703-871-8500
SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2100000001
Published Date: 10/7/20
Close Date: 10/14/20
Close Time: 13:30
Status: Closed
Solicitation Description: GRC Software Solution (OT21047)
Total of Header Attachments: 4
Total of All Attachments: 4

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder:	779602
Solicitation Description:	GRC Software Solution (OT21047)
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2020-10-14 13:30	SR 0231 ESR10142000000002966	1

VENDOR

000000195808
CARAHSOFT TECHNOLOGY CORP

Solicitation Number: CRFQ 0231 OOT2100000001

Total Bid: 999959.5699999999487772583961 **Response Date:** 2020-10-14 **Response Time:** 12:51:55

Comments:

FOR INFORMATION CONTACT THE BUYER
Jessica S Chambers
(304) 558-0246
jessica.s.chambers@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	GRC Software Solution				999959.57

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

See attached Pricing Page

carahsoft

CARAHSOFT'S RESPONSE TO THE

State of West Virginia: Department of Administration

Request for Proposal

GRC Software Solution

SOLICITATION NO. CRFQ OOT2100000001

Wednesday
October 14, 2020

SOLUTION PROVIDED BY

servicenow™

IMPLEMENTATION PARTNER:

edgile

CARAHSOFT TECHNOLOGY CORP.
11493 SUNSET HILLS ROAD, SUITE 100
RESTON, VA 20190

888.66.CARAH | WWW.CARAHSOFT.COM

October 14, 2020

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington St. E
Charleston, WV 25305-0130

Re: Carahsoft's Response to the State of West Virginia: Department of Administration's Request for Proposal for GRC Software Solution, Solicitation # CRFQ OOT2100000001

Dear Jessica S. Chambers,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of West Virginia: Department of Administration (DOA)'s Request for Proposal for a GRC Software Solution. Carahsoft is proposing ServiceNow Governance, Risk, and Compliance (GRC) software, which fully meets the DOA's requirements.

Since opening its doors in 2004, Carahsoft has successfully executed over 140,000 orders to State, Local Government, Educational entities. As a top-ranked partner for ServiceNow, Carahsoft has delivered best value solutions to our public sector clients for over 15 years.

Please feel free to contact me directly at 571-662-4206/ryan.veno@carahsoft.com or Jessica Robertson at 703-889-9725/jessica.robertson@carahsoft.com with any questions or communications that will assist the DOA in the evaluation of our response. This proposal is valid for 90 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Ryan Veno

Ryan Veno
Account Representative

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corp. is an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading software license GSA resellers.

VENDOR RELATIONSHIPS – Carahsoft has a unique business model focusing on providing superior sales and marketing execution, a track record of success, high integrity, and a focus on strategic vendor relationships, of which **ServiceNow** is an important part. Carahsoft's contract vehicles carry over 200 vendors. Carahsoft's unique ServiceNow qualifications include:

- Carahsoft is the sole Federal Distributor and GSA Schedule holder for ServiceNow products and holds the majority of contract vehicles supporting state, local, and higher education.
- Carahsoft has a dedicated sales team to coordinate with customers, resellers, and ServiceNow through the entirety of the purchasing process.
- Carahsoft has a deep understanding of both the government sphere and ServiceNow's product lines, which is critical to customer success and creating the best value for customers.
- Carahsoft has a dedicated ServiceNow marketing team to facilitate positive customer interactions through events, conferences, and webinars.

PROVEN EXECUTION – Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 94,000 orders in 2019 that were each completed the same day received.

CONTRACT VEHICLES – Since 2004, Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Associated with all contracts are dedicated and experienced contract management resources. A list of available contracts can be found at www.carahsoft.com/contracts/index.php.

GROWTH & STABILITY – Carahsoft has continued to show impressive growth year after year, with annual revenue of $3.4 million in our first year in 2004 to $6.6 billion in 2019. In September of 2019, 11,521 orders were processed worth nearly $1.4 billion. We are a stable, conservative, and profitable company and have received numerous accolades, as detailed on our awards page: http://www.carahsoft.com/awards.

- Top Ranked GSA Schedule 70 Contract holder for software
- #30 on Washington Business Journal's Largest Government Contractors List for 2016
- #40 on Washington Technology's Top 100 Government Contractors List for 2017
- Fed 100 Winner and Ernst & Young Entrepreneur of the Year, Craig P. Abod, President and CEO; Fed 100 Winner, John Lee, Vice President of Cloud Services

Solution Provider: ServiceNow

ServiceNow offers a comprehensive portfolio of cloud-based applications that create great experiences and unlock productivity across an organization. ServiceNow thinks of this Digital Transformation process and benefits in three distinct workflows.

1. Transform operational **IT** productivity
   - Standardize IT globally
   - Manage demand and resources better
   - Improve service availability
   - Reduce enterprise risk
   - Drive operational excellence through automation

2. Elevate **employee** experience
   - Enable employees with self-service
   - Improve HR productivity
   - Smooth employee on-boarding

3. Reimagine **customer** engagement
   - Increase customer satisfaction
   - Resolve issues faster
   - Personalize and predict

These workflows include the products listed below.

These workflows and applications are built on the ServiceNow Platform, which offers industry-leading infrastructure and architecture, integration, scalability, and security.

- **Architecture** – ServiceNow has a **game-changing architecture**. Many other cloud providers operate in a multi-tenant architecture (where many customers share the same database and application instance) and take their system down for planned maintenance more frequently and for longer time periods than ServiceNow. This impacts the cloud provider's ability to troubleshoot or perform maintenance on a single customer's instance without severely impacting many other customers. **ServiceNow offers a superior, single-instance architecture**; each instance has its own database and application set, allowing each customer to operate independently of other customers. ServiceNow compliments this with 18 data centers around the globe (nine pairs) that

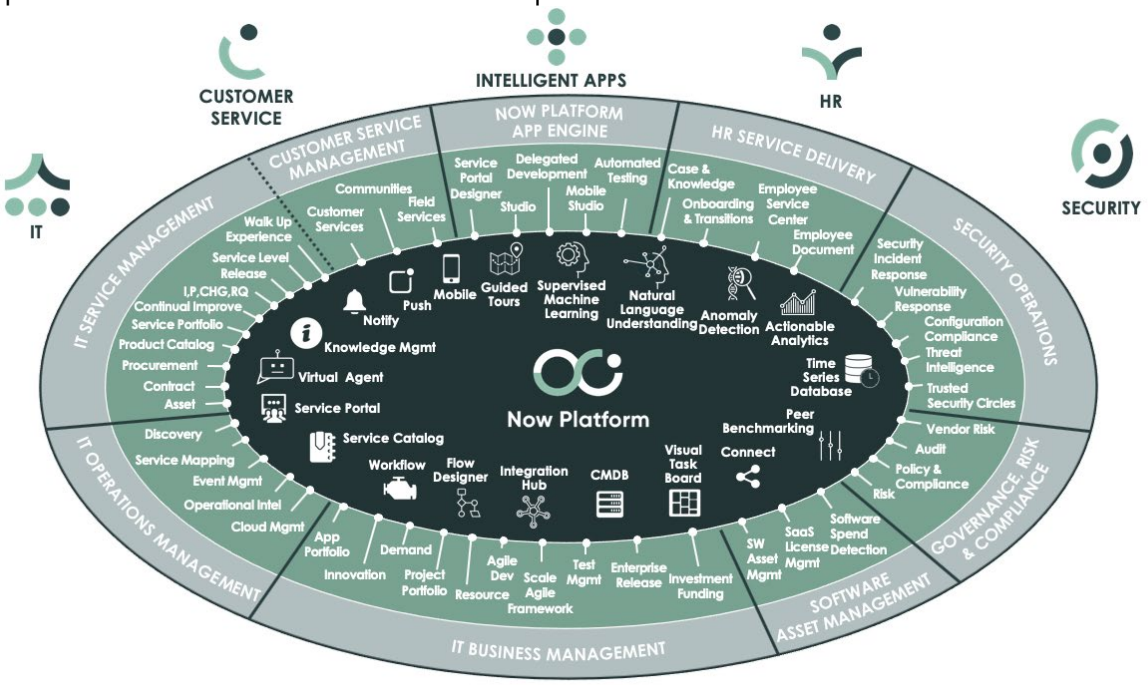
enable customers to fail over when issues arise or when ServiceNow is performing planned maintenance. When ServiceNow is working on an instance, a customer can still use it without seeing any change in performance.

- **Mobile Native** – With Now Mobile, employees and agents can find answers and get stuff done across IT, HR, facilities, finance, legal, and other departments—all from a modern mobile app powered by the Now Platform. Now Mobile provides:
  - **Native mobile for the enterprise** – Deliver tailored mobile experiences with an app powered by a single cloud platform with a common data model.
  - **Consumer-like mobile interface** – Make it easy for employees to get work done across departments without memorizing the corporate directory.
  - **Powerful self-help for all employees** – Enable employee self-service for better experiences and lower costs with Virtual Agent—native on the Now Platform.
  - **Consolidated approvals and to-dos** – Provide fast, easy access to common tasks across IT, HR, facilities, finance, and legal from a single location.
- **Integration** - All workflows and applications are built on a common platform, **eliminating the traditional challenges around data integration**. Any application on the ServiceNow Platform, including customer-built applications, can access and leverage all metrics, tasks, services, assets, people, locations, and information from a **single data source**, and everyone in the enterprise can access this information through a **single user portal**. All applications also leverage an **intelligent automation engine** to bring together people processes and automated processes. For more information on workflows and integration, please see the ServiceNow Platform Reference Guide.
- **Scalability** – ServiceNow is built on a **highly scalable, state-of-the-art cloud infrastructure**. With a clustered application and database server architecture, there is **no known limit** to the scalability of the ServiceNow implementation. ServiceNow has tens of thousands of customer instances operating globally in our data centers and over 150 million subscribed users. Customer instances perform an aggregate of tens of billions of full page transactions every month. Customers using the ServiceNow CMDB as the single system of record have scaled their CMDBs to manage tens of millions of configuration items (CIs). Our largest customer has tens of thousands of Fulfiller users and hundreds of thousands of Requester (end) users. We easily support all existing customers with room to grow and support customers large and small.
- **Security, privacy, and compliance** – ServiceNow understands that the security, privacy, and compliance are vital to all organizations, regardless of size. ServiceNow has achieved the US Federal Risk and Authorization Management Program Joint Authorization Board certification (FedRAMP JAB) **High level ATO and DoD Impact Level 4 authorization** enabling us to accelerate the adoption of secure cloud solutions by US Government agencies. The ServiceNow Platform provides industry-leading features and services – in a secure, reliable environment – that support customer implementations, as well as custom applications and application integrations. ServiceNow provides **24x7 operations and security monitoring** to help ensure customer instances are protected and operating as intended. We've engineered our cloud services, the infrastructure that supports it, our data **encryption techniques**, and **security threat response processes**, to ensure that the data is protected and secure at all times. For more information please see Securing the Platform: The ServiceNow Security Program Overview.
- **SaaS Solution** – Because ServiceNow is provided as a SaaS solution, there is **no client to install** to access the platform. The only requirement is a supported web browser and an Internet connection.
- **Configuration** – While much of the ServiceNow ITIL-based functionality is used as designed to be used out of the box, customer system administrators can configure ServiceNow using **no-code,**

low-code, and pro-code tools without the support of vendor or third-party consultants. Our innovative upgrade process allows the application of product releases, patches and hotfixes without negatively affecting configuration, helping ensure the long-term stability of any changes made by a customer. For more information on configuration, please see the ServiceNow Platform Reference Guide.

Platform Functionality

The solution described above is built on the Now Platform, a multi-instance cloud service infrastructure that is unparalleled in advanced high availability, "day one" compliance, and complete data security. The graphic below shows the breadth of ServiceNow platform.



Because all applications in the ServiceNow Portfolio are built on the Now Platform, all metrics, tasks, services, assets, people, locations, and information are stored together, creating a single system of record and a single system of engagement for the enterprise. All applications leverage the features listed below, including a common workflow engine to bring together people processes and automated processes. This allows work to flow seamlessly across all domain areas within an enterprise – automating tasks, consumerizing the service experience, and helping people work better and smarter. The Now Platform provides the following functionality:

- **Collaborate:** Connect, Chat, Coaching Loops, Live Feed, Visual Task Boards, Knowledge Management
- **Communicate/Integrate:** Email/SMS Alerts and Notifications, REST API, Native Mobile App, Web Services, OpenFrame, Import/Export
- **Manage Resources:** CMDB, Service Catalog, Timecards, Skills Management, Service Level Management, On-Call Scheduling, Role-Based Security
- **Intelligence:** Assessments, Automated Testing Framework, Reporting, Surveys, Business Service Maps, Visualizations, Google Maps, Contextual Search, Subscription Management, Visualizations

- **Design:** Content Management System, Delegated Development, Flow Designer, Form Designer, Graphical Workflow, Service Creator, Studio, Service Portal Design, Scripting, Script Debugger, Service Portal Designer

For more information on these functions, please see the ServiceNow Product Overview.

ServiceNow Customers
Thousands of customers world-wide use ServiceNow, including 43%+ of the Forbes Global 2,000, 50%+ of the Fortune 100 and many small- and medium-size organizations around the globe. Our customers span almost every industry from federal (civilian, DoD, and IC), finance, energy to education and managed service providers in 50 countries. According to Gartner, ServiceNow has 47% ITSM market share; approximately 30 businesses switch from legacy solutions to ServiceNow each month.

Implementation Partner: Edgile

Edgile is a specialized consulting firm consisting of senior experts in IRM/GRC, Identity and Cloud security. By only hiring experienced consultants and engineers, Edgile is a trusted partner to C-suite and Risk executives. Founded in 2001 and headquartered in Austin, TX, Edgile consists of approximately 180 employees located throughout the United States. In addition to working with State and Local Government Agencies, Edgile works with 45+ companies in the Fortune 500, including more than 12 in the Fortune 100. Over its history, the Edgile IRM/GRM Team has successfully executed hundreds of projects delivering solutions around:

- Authority Document Repository
- Risk Register
- Risk Assessment
- Control Testing
- Compliance Reporting
- Risk Reporting
- Issues and Finding Management
- Policy Lifecycle Management
- Business Hierarchy and Asset Definition
- Continuous Monitoring & KPI/KRI

Edgile has designed an organizational structure that enables it to assemble high performance work teams for each project. Each client engagement begins with the active participation of an Edgile senior partner, who works closely with a highly collaborative team made up of risk, compliance and governance professionals.

Edgile has been recognized by ServiceNow as an 'Elite' partner for implementing ServiceNow GRC because it understands the importance of integrating technology to enable business processes while providing a platform to automate and enhance capabilities. Our talent is exceptional; a few highlights include:

- ServiceNow Certified Implementation Specialist – Certified resources covering IRM/GRC, Vendor Risk Management, Business Continuity Management, Security Operations and the ServiceNow Platform.
- Professionals who have held senior leadership roles in industry (e.g., chief information security officer, chief risk officer, head of compliance and risk, head of governance) as well as practitioner

roles which gives the implementation team the necessary insight into designing, building and running programs.

- Development experts who have built ServiceNow Certified applications available at Store.ServiceNow.com, demonstrating our close relationship with the product team and an ability to develop solutions for our clients that are mindful of licensing and upgrade considerations.
- GRC practice members with experience in different industries (State and Local Government / Utilities / FSI / Health Sciences / Manufacturing) with an average of 10 years of experience.

PROPOSED SOLUTION

Qualifications

1. Vendor must have implemented a GRC software solution with a Federal or State, or Local Government entity and provide proof of implementation upon request.
Carahsoft will provide the relevant past performance documentation upon down selection or award of this proposal.

2. Vendor must hold current SOC 2 Type 2 certification.
ServiceNow is audited annually by a third party and has maintained its SSAE 18 SOC 1 Type 2 attestation since 2011 (SSAE 18 superseded SSAE 16 in 2017). SSAE 18 is aligned with international standard ISAE3402 and replaced the now-deprecated SAS70. ServiceNow has also undertaken an annual SOC 2 Type 2 attestation since 2013, relevant to security and availability controls listed in the AICPA Trust Services Criteria (TSC). A SOC 1 Type 2 bridge letter is provided between audit periods so that the company is covered for the entire year. This bridge letter is available via ServiceNow CORE to ServiceNow customers at the end of every January.

3. The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section 9.3.1.12 – Remote Access requirements.
Implementation consultant will remotely access the related ServiceNow SaaS Platform consistent with the State of West Virginia's treatment of the compliance requirements of IRS 1075 2016 (AC-17) including CE1, CE2, CE3, and CE4. For example, access over the internet to FTI will be performed using multi-factor authentication.

4. Vendor must appear in the Leaders quadrant of the Gartner's Magic Quadrant for IT Risk Management Report published August 11, 2020.
ServiceNow is named a Leader in the Gartner Magic Quadrant for IT Risk Management.
Read the full, complimentary report, https://www.servicenow.com/lpayr/gartner-it-risk-management.html, for

- A third-party, unbiased evaluation of vendor
- Insight into the significant movements in the market
- The factors driving growth

Software (4.1.1)

1. Vendors GRC solution must provide a cost-effective cloud-based Software-as-a-Service (SaaS) risk management solution for the State Cybersecurity Framework. (Including future scalability when new agencies are on-boarded).
The ServiceNow Governance, Risk, and Compliance (GRC) solution is provided as a SaaS solution. With a clustered application and database server architecture, there is no known limit to the scalability of the ServiceNow implementation. We continually test the scalability of our technology using internal testing tools and have experienced sub-second response times across a vast majority of transactions. Our largest clients have over 200,000 employees accessing the system every day, with over 30,000 people in the IT department. ServiceNow monitors and manages capacity from our centralized Network Operation Center, and adjusts capacity as necessary.

2. Vendors GRC solution must implement NIST Cybersecurity Framework (NIST CSF), NIST 800-53 control set, and align to PCI DSS, HIPAA, FERPA, CJIS, and other compliance programs.

ServiceNow GRC helps manage your governance framework, including policies, laws and regulations, and best practices in one system, and maps them to controls. Once defined, you can automate repetitive processes, even across functional groups. GRC customers can identify relevant business, risk and IT owners, and systems, and automate the manual cross-functional processes for policy lifecycle management and compliance testing to identify non-compliant controls, respond to issues, or effectively scope a GRC engagement. The unique capabilities of the ServiceNow platform help eliminate errors and inefficiencies associated with emails, phone calls, and in-person meetings. Additionally, using the built-in GRC Attestation Designer, you can create and execute tests and attestations that are specific to a policy statement. This helps eliminate errors during evidence data collection and mitigates the need to manually reconcile test results and metrics.

In terms of built in templates, ServiceNow contains templates for SOX, NIST RMF and NIST CSF. Additionally, we have a partnership with the Unified Compliance Framework, which would allow for content on regulations and industry best practices to be brought in automatically into the ServiceNow GRC solution.

For further information, please refer to the following links:

https://store.servicenow.com/sn_appstore_store.do#!/store/application/d8a58b32d7221200d77c83e80e6103b4/7.0.7?referer=sn_appstore_store.do%23!%2Fstore%2Fsearch%3Fq%3Ducf.

https://docs.servicenow.com/bundle/newyork-governance-risk-compliance/page/product/grc-policy-and-compliance/reference/r_PolicyComplianceMgmt.html

3. Vendors GRC solution must automatically implement changes or updates in laws or compliance programs and alert users to relevant updates.

You can update the UCF documents you use in GRC manually or configure the system to do it automatically whenever a new UCF version is available.

By default, GRC downloads the most recent version of the UCF authority documents, which are updated quarterly. The ServiceNow system places these files in staging tables until they are imported into GRC. When you import a new document version, these entities are updated:

- Authority documents
- Citations
- Controls

GRC observes these general rules when importing updated documents from UCF:

- If UCF authority documents or citations are updated, both entities are imported into GRC and versioned.
- If only the UCF controls are updated, then only the controls are versioned. In this case, a new link is created between the updated control and the existing citation that uses it.
- Older versions of updated controls are automatically deactivated and do not appear in lists of controls.

The control test definitions, policies, and risks that use these updated entities are reset to use the latest version. Any control test instances tied to a control from the previous version remain linked to that control. You must generate new control test instances based on the latest UCF version. The system deactivates all previous versions of an imported UCF document and retains them in their respective GRC tables.

4. Vendors GRC solution must maintain the Security Requirements Traceability Matrix (including objectives, risks, controls, ranks, rates, etc.), and allow periodic updates to be made.

Governance, risk, and compliance (GRC) is a general term describing the combination of people, processes, and products involved in establishing and executing business goals, while mitigating risk and proving compliance with regulations.

The Governance, Risk, and Compliance (GRC) application supports:

- Creating policies
- Defining and assessing risks
- Defining controls based on policies and their associated risks
- Downloading and importing Unified Compliance Framework (UCF) data. See https://www.unifiedcompliance.com/.
- Generating audits and tests to ensure that controls are being followed
- Generating remediation tasks to track corrective actions that are required

5. Vendors GRC solution must identify and assess strategic risks, opportunities, and mitigating controls.

The Governance, Risk, and Compliance (GRC) application supports:

- Creating policies
- Defining and assessing risks
- Defining controls based on policies and their associated risks
- Downloading and importing Unified Compliance Framework (UCF) data. See https://www.unifiedcompliance.com/.
- Generating audits and tests to ensure that controls are being followed
- Generating remediation tasks to track corrective actions that are required

6. Vendors GRC solution must monitor and manage strategic risks and opportunities.

Risk management enables an organization to quickly identify and quantify the impact that loss events affecting various business processes and items (such as facilities, business services, and vendors) pose to the organization.

The risk library contains all risk frameworks and risk statements. Risk frameworks are used to group risk statements into manageable categories, while risk statements group the individual risks. The risk register is the central repository for all potential risks that could occur at anytime, anywhere in the organization.

Assessing risk means identifying and analyzing the threats and vulnerabilities that could adversely affect your organization's business objectives. Risk is a function of the likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. By identifying your risks and the impact and likelihood of those risks occurring, your organization can prioritize control testing and remediation activities. It also helps you understand the true business impact when a control fails.

7. Vendors GRC solution must report strategic risks and opportunities.
The Operational Risk Management dashboard enables an authorized user to view the complete risk posture for the enterprise in a single consolidated report. This dashboard makes it easy to analyze the risk posture efficiently and take necessary corrective actions to ensure that there are no losses. For more information, please see https://docs.servicenow.com/bundle/paris-governance-risk-compliance/page/use/dashboards/application-content-packs/operational-risk-dashboard.html.

The GRC Application Risk and Compliance Overview Dashboard provides the latest view of risk and compliance aspects for the business applications that are used in an enterprise. For more information, please see https://docs.servicenow.com/bundle/paris-governance-risk-compliance/page/product/grc-common/concept/advanced-grc-dashboard.html.

8. Vendors GRC solution must include a workflow management component that allows for work to be created and shared (internally or externally), including the ability to record user comments.

ServiceNow provides a robust workflow engine that uses role-based entitlements, and administrators can grant entitlements to roles with the explicit need for the level of access.
We provide out-of-box workflows that can be leveraged/configured to get started and meet your specific requirement(s). A typical use case include workflows for vendor tiering assessments and periodic vendor assessments.

Additionally, with the ServiceNow Flow Designer, a Platform® feature for automating processes in a single design environment, it is possible to design new workflows and implement them without any coding. Flow Designer lets process owners use natural language to automate approvals, tasks, notifications, and record operations without coding. With Flow Designer you can:

- Create flows and actions and manage flow execution in a single environment.
- Enable automation and speed up development by creating reusable content available to any flow.
- Improve upgrades and maintenance by replacing customized business logic with native Now Platform actions.

9. Vendors GRC solution must automatically push out control assessments to control owners annually.
Authorized users can define how frequently the reassessment must be performed. The choices are:

- None
- Weekly
- Monthly
- Quarterly
- Semi-annually
- Annually

This process provides visibility and accurate reporting for the management.

10. Vendors GRC solution must send reminders/receive feedback on due tasks and dates to all relevant resources and other stakeholders.

The ServiceNow platform can email selected users automatically about specific activities in the system, such as updates to tasks or upcoming due dates. Email notifications allow administrators to specify:

- When to send the notification
- Who receives the notification
- What content is in the notification

Users can also choose whether to receive email notifications by setting a preference on their user record. If the Subscription-Based Notifications plugin is active, additional email notification options are available. Users can subscribe to notifications and administrators may make some notifications mandatory.

For further information, please refer to the following link: https://docs.servicenow.com/bundle/paris-servicenow-platform/page/administer/notification/reference/notifications.html.

11. Vendors GRC solution must deliver automated escalations if deadline is approaching.

You can use the escalation feature to highlight specific cases or accounts and raise awareness of important customer issues. Escalating cases or accounts facilitates communication about an issue and enables users to track progress toward a resolution. An escalation provides increased attention to a customer issue and provides a way to track the progress made in resolving the issue. Escalation is an internal process that is not exposed to customers. Users with the escalation_requester role can escalate cases or accounts on behalf of customers or for internal purposes.

The escalation process can include an optional approval step where approvers review the request and either approve or reject the escalation. When an escalation is approved, an escalation record is created and is associated with the case or account. Agents and escalation managers can manage the case or account through the escalation process using the escalation record. Escalated cases and accounts are identified on lists and forms with color indicators that correspond to the escalation severity.

Users with the de-escalation requester role can de-escalate cases or accounts when the cause of the escalation is resolved. While the escalation process is similar for cases and accounts, there are some important differences to note between case escalations and account escalations. A customer service agent typically manages a case escalation and works directly with the escalated case to resolve the issue. An escalation manager typically manages an account escalation, which can include multiple associated cases, and records details in the escalation record

All escalations can be configured to be automatically triggered based on a deadline.

12. Vendors GRC solution must provide standardized templates for different functions/areas, including reporting templates and a testing result reporting template linked to every control.

Users of governance, risk, and compliance can view reports on attestations, compliance, controls, and audits. The GRC reporting portals provide reports to specific users related to the GRC elements assigned to them or their groups.

GRC provides portals that deliver reports to specific users related to the GRC elements assigned to them or their groups. Those reports include the following information.

- Overview of all UCF document import activity.

- GRC related tasks and assessments assigned to the logged in user, the user's group, or people who report to the logged in user.
- Time remaining on time-sensitive GRC elements.
- GRC update approvals for the logged in user.
- Progress on tasks, including subtasks completed versus those remaining.
- Results filtered by audit, department, company, individual, type, and group

13. Vendors GRC solution must allow for documentation of risk/control issues/findings/remediation plans.

ServiceNow supports the entire problem management lifecycle from first identification through investigation, documentation, and removal. To proactively prevent incidents, staff reviews reports for service performance trends and reviews service configurations in the ServiceNow Configuration Management Database (CMDB) to identify potential failures. To help identify the true cause of a problem, staff can follow a structured problem analysis methodology to avoid making wrong decisions based on subjective opinions. When errors and workarounds are identified they are published in the ServiceNow Knowledge Base. During an incident, workarounds are communicated to affected parties and stakeholders through Problem Management or Incident Alert Management. Remediation plans to permanently remove errors are scheduled through ServiceNow Change Management. To minimize the impact of incidents that cannot be prevented, ServiceNow Coaching Assessments monitor critical moments of a process in real-time giving coaches the opportunity to quickly intervene to correct any mistakes that could cause more trouble or delay service restoration. This can all be captured in a Knowledge Base article and is integrated in the CMDB.

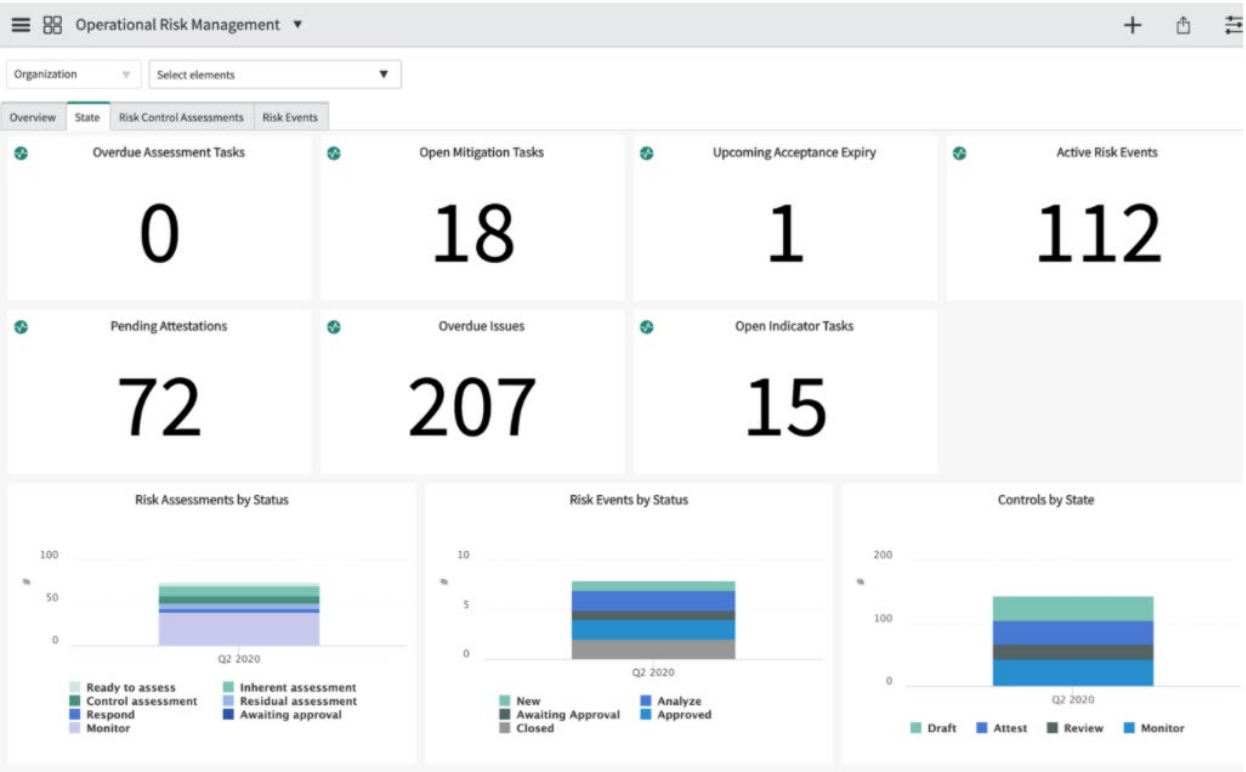
14. Vendors GRC solution must track remediation deadlines/timelines.

Remediation within the platform can be tracked within Issues Management. This allows items required for remediation to be tracked, assigned to owners, and reported upon. The customer can also define the workflow in terms of the required tasks, approvals and information for closure. Reports and dashboards can be generated based on any data elements included as part of the issue record itself.

For further information around issues management, please refer to the following link:https://docs.servicenow.com/bundle/paris-governance-risk-compliance/page/product/grc-risk/concept/issues-risk.html

15. Vendors GRC solution must provide a dashboard to show, at a minimum, which updates are outstanding, the last Security Requirements Traceability Matrix review dates, and when testing is overdue.

https://docs.servicenow.com/bundle/paris-governance-risk-compliance/page/use/dashboards/application-content-packs/operational-risk-dashboard.html



16. Vendors GRC solution must provide data visualization tools or allow export of data to other tools such as Microsoft Office

ServiceNow provides native reporting tools that can consolidate any information on the platform. Built on a centralized single data model with advanced reporting functionality, ServiceNow engine helps you instantly retrieve and share up-to-date information in the shortest amount of time. It also includes 200+ predefined reports, visualizing data across many ServiceNow applications and features. You can generate ad hoc reports and save, share, publish, or export them as needed. Report types include lists, charts, geo-maps, scores, or calendar-based views of data in a particular table. If none of the predefined reports meet your needs, you can also create your own custom reports, as well as add reports on home pages and dashboards to share information across your organization. Reports can be saved and shared via email or via the Service Portal. Reports can also be exported to the following formats:

- PDF: Displays as a Portable Document Format (PDF) file in either portrait or landscape orientation. PDF reports include the chart grid data.
- Excel: Displays as a Microsoft Excel spreadsheet.
- PNG: Displays as a Portable Network Graphic (PNG) file.

17. Vendor must provide a means to summarize and track data in the system.

Visual task boards transform the navigation of lists and forms into an interactive graphical experience. They allow users to view and update multiple task records, which appear as cards that can be moved between lanes. An activity stream on the board displays recent activity so users can easily track changes to tasks. You can add task cards from any table that extends Task to intuitively and easily track updates and edit records directly from the board. Any user, regardless of role, can use task boards but can only see cards for records the user has access to. The visual task board interface provides a graphic-rich environment

suited for managing and collaborating on records. For example, a support manager might create a board for her team to track their assigned incidents by state in real time.

18. Vendor must provide a means to summarize performance metrics.

Customers can view a wide range of performance metrics for their instance and for the machine on which your instance is running, displayed in a graphical format. Administrators can add these graphs and their controls to a home page to monitor the performance of instances. Some of these graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues or help customers tune the system for maximum efficiency. Each graph enables users to filter the data by using different measurements, such as maximum and minimum values, means, and medians. The available graphs reflect performance in eight functional areas of ServiceNow.

- Database
- Discovery
- Disk Partitions
- Linux Stats
- Logging
- MySQL Overview
- Node Metrics
- Replication
- ServiceNow Servlet

Database graphs, available to view on the Performance homepage, display metrics for various database operations, for example, insertions and deletions. They also display a current count of database connections for the selected ServiceNow instance.

19. Vendors GRC solution must have user/access management tools to allow for creation/management of user accounts (Active Directory integrated preferred for future use; role-based access required)

a. Role-based access must be defined at the functional level (i.e. allow user access to data only relevant to their function)

b. Will restrict certain functions to authorized staff only (i.e. certain user group has read-only access, another user group has ability to delete records)

Implementation consultants will work with the State of West Virginia project stakeholders to define the business, functional and technical requirements including but not limited to user/access management. Specifically, the requirements to integrate with Microsoft Active Directory (AD) and related role-based access control will be defined, configurations made, and user acceptance testing performed until defect-free. This includes ensuring that role-based access is defined at functional levels (e.g., control owner, risk assessor, risk assessment manager, etc.) to enable entitlements which grant access to the data only relevant to their function. Further, certain functions will be more granularly defined to allow only authorized staff to create, read, update, associate, and delete specific records and/or fields.

ServiceNow uses role-based entitlements, and administrators can grant entitlements to roles with an explicit need for the level of access. Access to applications, modules, reports, platform features, and data is controlled by assigning users to roles and then granting role-based access using access control lists (ACLs). Security rights within ServiceNow are controlled using granular ACLs, which can secure

information table by table, row by row, or attribute by attribute based on role, group, department, location, or other criteria.

20. Vendor solution must include ability to help manage the incident management process including the use of templates, automated workflows, and dashboards.

The ServiceNow Security Incident Response application can manage the entire lifecycle of the security incident from detection to closure.

- Detection: Security incidents can be created within the ServiceNow platform in a variety of ways. Many customers integrate ServiceNow with their SIEM solution, either through out-of-box integrations, including Splunk, ArcSight, QRadar, and McAfee ESM, or through configuration of an API. Additionally, incidents can be manually created by analysts or end users through the use of a security catalog. Lastly, emails can be forwarded to the ServiceNow platform (such as possible phishing emails) to initiate the incident process.
- Analysis: The security incident will be given a risk rating dependent on both the severity of the alert and the criticality of the asset affected. The incident can then be triaged and assigned to the appropriate individuals on the security team. Once that is completed, the incident can be enriched with any threat intelligence feeds gathered by the customer.
- Recovery: Once the incident has been triaged, the appropriate workflows in ServiceNow can be initiated to assign response tasks and items associated with the specific requirements of the incident. ServiceNow Workflows automate multi-step processes that occur between any combination of people and systems to help companies achieve better business outcomes. Our approach to workflow removes bottlenecks and integrates processes and activities between people and systems. Interactions that involve forms, requests, approvals, and events can be simplified with automated workflows using a drag-and-drop interface that visualizes the entire sequence of activities in an easy-to-understand flowchart. Activities can include anything from generating records and notifying users of pending approvals to running timers, tasks, scripts, and more. You can create end-to-end automation of the previously manual or disconnected processes that drive your business. More than 20 out-of-box workflows are templated, and these can be modified and adjusted to a customer's needs.
- Post-Incident: Once the proper tasks have been completed, a post-incident assessment can be sent out to all involved analysts to perform a lessons-learned exercise. Additionally, these results can be compiled within a final report.

Implementation/Services (4.1.2)

21. The vendor must conduct training with a group of at least fifteen (15) power users of the new tool enabling a "train- the- trainer" approach.

Implementation consultants will develop and deliver two-types of training: one for management or power users and another for end-users of the solution. The training includes development of step-by-step guidance with corresponding screen shots directly from the 'as-built' solution. Training will be delivered in both a Microsoft PowerPoint format for use following the project, as well as delivered via video conference/collaboration software (e.g., Teams, Zoom, WebEx) to a live-audience to further enable a "train-the-trainer" approach desired by the State of West Virginia.

22. Additionally, tool must provide online on-demand, self-paced training.
In addition to the dual-audience training identified in section 4.1.2 point 21 which the implementation consultant will provide, ServiceNow has numerous online, on-demand, self-paced training that can be taken by professionals within the State of West Virginia. While some of these online training courses are offered at no cost, some are offered at a nominal cost (e.g., some training courses leading to certification).

23. The vendor must provide technical support within one (1) business day and make best efforts to resolve problems as quickly as possible.
During the project to setup and configure the solution, the implementation consultant will provide technical support within one (1) business day, making best efforts to resolve problems as quickly as possible.

24. The vendor must guarantee application has 99.9% uptime.
The implementation consultant will capture the related business, functional and technical requirements specifying 99.9% uptime and configure the solution consistently with that objective. That said, the ServiceNow SaaS Platform uptime target is defined and managed by ServiceNow and included as part of the licensing agreement between ServiceNow and the State of West Virginia.

ServiceNow offers an SLA for solution availability; the solution will have 99.8% availability for production instances, calculated monthly. Please see the Subscription Service Guide for information on this availability SLA. Please see the Exhibit A.2 Customer Support Policy, in the Subscription Service Guide, for information on response time.

25. The vendor must provide frequent progress reports during any outage.
The implementation consultant will provide progress reports, minimally daily but likely more frequently, in the even an outage occurs during the project. Furthermore, ServiceNow will provide progress updates regarding outage resolution for the platform as a part of their SaaS offering.

Customers can track the status of all requests through the Customer Support portal ("Support Portal") (ServiceNow uses our own solution to manage support requests). Please see the Subscription Service Guide Exhibit A.2 Customer Support Policy for details.

26. The vendor must ensure that State of West Virginia data is not co-mingled with other customer's data.
The implementation consultant will capture the related business, functional and technical requirements specifying that the State of West Virginia's data not be co-mingled. As a matter of protocol, the instances of ServiceNow that would be envisioned supporting the State of West Virginia would be provided in a manner that prevents the State of West Virginia's data from being co-mingled with other customer's data. To the extent related configuration is required to achieve the objective, the consultant will configure ServiceNow accordingly.

Each instance has a single database present on a database server running multiple discrete databases. There is no commingling of any customer data between instances and databases, nor shared multi-tenant databases with data from multiple customers stored therein. For example, if a customer has four instances of ServiceNow, they will have four entirely separate databases and database services, one unique to each

instance. These database services may run on different database servers and there is no assumed relationship.

27. The vendor must ensure that State of West Virginia data can be exported and returned to the state.
ServiceNow has several options for an exit management plan. At least thirty (30) days prior to either the expiration of the Subscription Term (where the customer elects not to renew) or in connection with the termination by the customer of the Subscription Service in accordance with ServiceNow's General Terms and Conditions, the customer may purchase the following services: (i) one (1) extension of the Subscription Service for up to six (6) months ("Transition Subscription Service"); and (ii) Professional Services. The customer pays in advance for the Transition Subscription Service at the monthly subscription fee rate charged to the customer in the expiring Order Form plus an additional ten percent (10%). The customer pre-pays for any Professional Services ordered during the transition period plus verifiable travel and expenses. The parties sign a mutually agreed upon Order Form setting forth the fees and purchased Subscription Service and Professional Services prior to the commencement of any Transition Subscription Service or Professional Services. ServiceNow can provide customer data in its standard database export format. The process for the return of data follows:

- ServiceNow exports the entire database in a standard database export format.
- ServiceNow provides the customer a set of instructions on how to import the data on the customer's side.
- The customer can FTP the files from ServiceNow to their site. Customers are permitted to store data hosted within ServiceNow for the duration of their service subscription with ServiceNow. Under this model, the customer can purge or retain data according to their own retention policy. ServiceNow retains customer data for up to 45 days from the end of a contract. Within the 45 days, the customer can request their data to be sent to them in a standard database export format. After 45 days, all data from the customer instances is removed from ServiceNow servers.

28. The vendor must ensure State of West Virginia data is destroyed at the end of the contract.
After 45 days, all data from the customer instances is removed from ServiceNow servers. Please see answer to number 27 above.

29. Vendor must support data in transit encryption using TLS 1.2 or higher.
The implementation consultant will capture the related business, functional and technical requirements specifying TLS 1.2 or higher for transmission encryption, and the implementation consultant will configure the ServiceNow platform to use TLS 1.2 or higher to support data in transit encryption, consistent with the design and intended use of the ServiceNow platform.

Normal user traffic from a browser to ServiceNow is encrypted by default over TLS 1.2.

30. Vendor must support encryption at rest using AES-256 or higher.
The implementation consultant will capture the related business, functional and technical requirements specifying AES-256 or higher for encryption of data at rest, and the implementation consultant will configure the ServiceNow platform to use AES-256 or higher to support data encryption at rest, consistent with the design and intended use of the ServiceNow platform.

ServiceNow uses self-encrypting hard drives (for full-disk encryption) to protect the confidentiality of customer data at rest. Full-disk encryption is implemented by default in ServiceNow's U.S. Federal/Government data centers and is available in commercial data centers for an additional cost. The drives use an encryption key generated by a SafeNet appliance, utilizing a FIPS 140-2 validated cryptographic module. The self-encrypting hard drive model used by ServiceNow in the FedRAMP environment is also FIPS 140-2 Level 2 validated and uses AES-128 to protect data.

31. Vendor must use two-factor authentication and or network access control limiting access from an exposed IP or subnet preferred.
The implementation consultant will capture the related business, functional and technical requirements specifying two-factor authentication and/or network access control, and the implementation consultant will configure the ServiceNow platform to use either two-factor authentication and/or network access control limiting access from an exposed IP, consistent with the design and intended use of the ServiceNow platform.

Implementation Timeline

Edgile has implementation accelerators specifically tailored to ServiceNow IRM/GRC which help deliver quick wins and provide our clients with high-value capabilities with a faster time to value.
A few key accelerators Edgile frequently uses with clients similar to the State of West Virginia is our Automated Regulatory Compliance (ArC) Content subscription for State and Federal Government Agencies along with the corresponding Regulatory Change Management solution. These two accelerators are designed to merge with clients' existing risk and control frameworks, simplify risk and compliance management, and enable an organization to create and customize its own control frameworks with full linkage back to relevant authoritative mandates such as NIST Cybersecurity Framework (NIST CSF), NIST 800-53 Rev. 4, PCI DSS, 45 CFR 160 (HIPAA), FERPA, and other compliance programs.

To this end, Edgile envisions performing the following summary activities as part of the solution implementation (with related RFQ citations noted):

- Week 1 – Define business, functional and technical requirements in partnership with the State of West Virginia.
- Week 2 – Review and refine the requirements based upon stakeholder feedback; develop the corresponding user acceptance test plan that will be used by the State of West Virginia to demonstrate their objectives for the solution have been successfully met.
- Week 3 – Begin configuration of ServiceNow to include integration with Microsoft Active Directory (AD), and two-factor and/or network access control configuration and calibration. Obtain the Edgile Automated Regulatory Compliance (ArC) Content and Regulatory Change Management solutions from the ServiceNow Store; facilitate the source selection process to determine which mandates are to be included in the State of West Virginia's integrated risk and compliance content library (e.g., NIST CSF, PCI DSS, etc.)
    - RFQ 4.1.1.19
- Week 4 – Begin configuration of fields, relationships, forms and portals, and other related UI/UX matters. Also begin the configuration of risk assessments, control testing, issues and remediation plan management, the ArC Content, and the Regulatory Change Management solution. This

includes ensuring the Security Requirements Traceability Matrix (including the objectives, risks, controls, ranks, rates, etc.) can be maintained and periodic updates facilitated.
    - RFQ 4.1.1.2, 4.1.1.3, 4.1.1.4, 4.1.1.5,
- Week 5 – Begin configuration of reports and dashboards; performance metrics related to control testing and Security Requirements Traceability Matrix reviews; as well as configuration of issues/findings/remediations plans.
    - RFQ 4.1.1.7, 4.1.1.12, 4.1.1.13, 4.1.1.14, 4.1.1.15, 4.1.1.16, 4.1.1.17, 4.1.1.18
- Week 6 – Begin configuration of role-based access control. Preview the 'as-is' build with the State of West Virginia, identify potential changes to be made (e.g., changes to field layout, risk and control solutions, UI/UX, etc.)
    - RFQ 4.1.1.19
- Week 7 – Begin configuration of workflows and notifications. This includes automated escalation if a deadline is approaching and work is unfinished.
    - RFQ 4.1.1.8. 4.1.1.9. 4.1.1.10, 4.1.1.11, 4.1.1.20
- Week 8 – Complete outstanding configuration tasks.
- Week 9 – Support the State of West Virginia's performance of user acceptance testing (UAT).
- Week 10 – Perform potential defect resolution and support re-performance of UAT until defect free.
- Week 11 – Prepare training materials for both management (train-the-trainer) and end-user audiences.
    - RFQ 4.1.2.1
- Week 12 – Deliver the training to two audiences: management and end-users.
    - RFQ 4.1.2.1
- Week 13-16 – Consultant to provide 1 FTE ServiceNow developer for 4-weeks of support to assist in migration of the solution from the development environment to higher environments such as production, as well as perform ad-hoc enhancements to the platform as directed by the State of West Virginia.

PRICING

Please see attached excel for software and implementation pricing.

Price notes:

1. Included in the price table is base year plus three one year options for subscriptions, implementation and training credits in the base year for the initial configuration, and 200 hours of post implementation each year for configuration changes.
2. Subscription pricing in each option year assumes all quantities of each product ordered initially are renewed. Currently scoped is ServiceNow IRM Pro (75); FedRAMP Instance (2); IntegrationHub Starter (1); ITSM Pro (2); learning credits (72).
3. Annual renewals after the initial offer and option years may incur up to 10% uplift.
4. The end customer's access and use of the Subscription Offerings are pursuant to the Public Sector Subscription Terms of Service, Customer Support Addendum, Data Security Addendum, Data Processing Addendum, Product and Use Definitions, Product Overview, and where applicable, the Service Descriptions for any purchased packaged professional services published as of the effective date of this Order Form at: https://www.servicenow.com/upgrade-schedules.html ("ServiceNow Subscription Service Terms"). ServiceNow Subscription Service Terms ARE EXPRESSLY DEEMED INCORPORATED HEREIN BY THIS REFERENCE.
5. Implementation costs have been estimated based on the requirements provided in the RFP. It is recommended a technical call be conducted to confirm the scope of the effort, resulting in a more accurate implementation price.

CONTRACTUAL CAVEATS

Carahsoft does not negotiate terms during the initial RFP process, but upon down-selection, we will work together with the State to arrive at mutually beneficial terms.

Carahsoft will also comply with the State's requirement for a purchasing affidavit, which we will complete and provide to the State upon down-selection.

Please see below comments related to the Software as a Service Addendum terms.

3c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.

Yes, as long as they can use one of our integration methods, see below:

Authentication and Authorization are primary components of the system, and these are enforced throughout the ServiceNow platform. Authentication can use several different methods to authenticate users.

- Local database: The user name and password is stored in their user record in the instance database. Passwords are hashed using a salted SHA256 algorithm.
- LDAP: The user name and password from their LDAP account, which has a matching user account in the ServiceNow database.
- SAML: The user name and password configured in a SAML identity provider account, which has a matching user account in the ServiceNow database.
- OAuth 2.0: The user name and password of OAuth identity provider, which has a matching user account in the database. This is used when using the ServiceNow mobile app.
- Digest Token: An encrypted digest of the user name and password in the user record.

For Local Database and LDAP authentication, the customer can enable multi-factor Authentication (MFA), requiring the user to enter in a pin in addition to their password, thereby creating strong authentication. The user(s) would enter a pin from Google Authenticator that was available on the user's mobile device.

For customers that have multiple identity providers, there is the option of Multiple Provider SSO, allowing you to choose to use several identity providers (IdPs) to manage authentication as well as retain local database authentication. You can use SAML and Digest Authentication through the Multiple Provider SSO application.

Each User Record can only have one Authentication method enabled for that specific user. However, the flexibility of having multiple authentication options allows an organization to choose what method is right for each person needing access to their ServiceNow application.

Authorization is accomplished with features such as Filters, ACLs, Query Rules, Domain Separation, and Separate Instances.

3d) PCI DSS

This is not applicable to the scope of this solicitation.

5. Breach Responsibilities
ServiceNow recommends customers encrypt sensitive data. Several encryption options are available. Refer to ServiceNow document *Security the Platform – The ServiceNow Security Program Overview*, for additional details.

Service recommends opening a P1 ticket if a breach occurs, which yields a 30 minute response to any breach.
https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/customer-support-addendum-upgrades.pdf

Please also refer to the attachment entitled "*Securing the Platform – The ServiceNow Security Program Overview"* for more information regarding security breach procedures.

ServiceNow provides terms and conditions for the use of the subscription service. Breach is defined in the Data Security Addendum (https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/data-security-addendum.pdf), sections:

5.1.2. BREACH NOTIFICATION. ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "Breach") without undue delay following determination by ServiceNow that a Breach has occurred.

5.1.3. REPORT. The initial report will be made to Customer security contact(s) designated in ServiceNow's Support Portal (or if no such contact(s) are designated, to the primary technical contact designated by Customer). As information is collected or otherwise becomes available, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected individuals, government agencies, and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform Customer of the measures that ServiceNow will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.1.4. CUSTOMER OBLIGATIONS. Customer will cooperate with ServiceNow by providing any information that is reasonably requested by ServiceNow to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

8. Background Checks:

Confirming that Edgile performs background checks consistent with W.Va. Code §15-2D-3 and include the State's 'e-Verify' eligibility checks which will be performed for resources assigned to the project supporting the State of West Virginia; the service provider will promote and maintain an awareness of the importance of securing the public jurisdiction's information among our employees and agents. Further, per requirement

#8, any resource that may be disqualified per the State of West Virginia's criteria (e.g., felony conviction) will not be part of the project.

10. Access to Security Logs and Reports

They do this in their system.

11. Data Protection Self-Assessment

ServiceNow will be able to fulfill this requirement, but the State will need an NDA to receive the assessment.

18. Subcontractor Compliance

Confirming that Edgile, should any subcontractors be engaged, will ensure those subcontractors have positively confirmed their agreement and compliance with the terms and conditions applicable to a service provider as outlined in the Software as a Service Addendum.

19. Right to Remove Individuals

Confirming that Edgile will remove, at the State of West Virginia's direction, any service provider representative believed to be detrimental to the working relationship.

IN SUMMARY

Carahsoft Technology Corporation and ServiceNow appreciate the opportunity to offer this solution for the DOA's initiative.

The Carahsoft Team has proposed a superior and cost-effective solution that fully complies with the DOA's requirements set forth in Solicitation # CRFQ OOT2100000001. We understand the importance of your project goals, and we are confident you will benefit from this solution and our expertise.

Carahsoft looks forward to the opportunity to speak with you regarding the details of this proposal, as well as the opportunity to work with State of West Virginia: Department of Administration on this project.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: OOT2100000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

☑ Addendum No. 1	☐ Addendum No. 6
☑ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Carahsoft Technology Corporation

Company

Jessica Robertson

Authorized Signature

10/14/20

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Contract Manager:	Jessica Robertson
Telephone Number:	703-889-9725
Fax Number:	703-871-8505
Email Address:	jessica.robertson@carahsoft.com

EXHIBIT A – Pricing Page
GRC Software Solution RFQ - OT21047

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1, 4.2	Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	541925.25	$ 541,925.25
4.1.3	Contract Item #2: Post Implementation Customization	HR	200.00	209.68	$ 41,936.00
4.1, 4.2	Optional Renewal Year 2: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	96763.44	$ 96,763.44
4.1.3	Optional Renewal Year 2: Contract Item #2: Post Implementation Customization	HR	200.00	209.68	$ 41,936.00
4.1, 4.2	Optional Renewal Year 3: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	96763.44	$ 96,763.44
4.1.3	Optional Renewal Year 3:Contract Item #2: Post Implementation Customization	HR	200.00	209.68	$ 41,936.00
4.1, 4.2	Optional Renewal Year 4: Contract Item #1: Governance, Risk, and Compliance (GRC) Software Solution, Training and Support	LS	1.00	96763.44	$ 96,763.44
4.1.3	Optional Renewal Year 4:: Post Implementation Customization	HR	200.00	209.68	$ 41,936.00
		Total Cost		$	999,959.57

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor Signature: **Date:**

Securing the Now Platform

The ServiceNow security program overview

servicenow™

START »

Introduction

ServiceNow provides a cloud-based platform and solutions that deliver digital experiences that help people do their best work. Our applications automate, predict, digitize, and optimize business processes and tasks across the enterprise.

This white paper describes ServiceNow's security program across a number of key security domains. These include architecture, information lifecycle, physical security, security operations, disaster recovery and business continuity, privacy, compliance, and software development. All these domains are represented from the context of ServiceNow as both a software vendor and as an operator of a large private cloud infrastructure.

While this white paper can serve as a standalone summary of the ServiceNow security program, by design it forms part of the ServiceNow Trust Journey, which leads up to this summary.

Definitions and context

The ServiceNow environment is a private enterprise cloud service, fully owned and operated by ServiceNow. This cloud features a "multi-instance" architecture that delivers logical single tenancy by isolating all customers' data from each other. This is achieved by utilizing an enterprise-grade cloud architecture and a dedicated database and application set per customer instance—there is no combining of data or other forms of multi-tenancy.

ServiceNow cloud

ServiceNow instances operate on a single cloud platform that consists of one user interface, one code base, a common API, and one data model. This is supported by a global support organisation, operating to a single set of processes and tools, under a common governance and compliance structure. Having a single product, platform, and support infrastructure means that ServiceNow can employ extensive security without the need to balance security over a highly diverse estate.

ServiceNow customers obtain the benefits of shared infrastructure, while taking advantage of the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each instance, customers can access additional security features within their ServiceNow instances.

The Now Platform

The Now Platform® is a powerful cloud application platform that enables customers to link real-time data with activities, tasks, and processes to achieve better work outcomes. Further information can be found at https://www.servicenow.com/now-platform.html.

Instance

An instance is an entirely discrete ServiceNow environment consisting of two or more application nodes and a single database which stores all data, code, and configuration data for the instance. Production instances are automatically replicated to passive data centers, whereas sub-production instances only exist in a single data center.

Information security governance and risk management

Security frameworks

ServiceNow's security framework is based on ISO/IEC 27002:2013. As an ISO/IEC 27001 certified organization there is a high level of integration between the ISO/IEC 27002:2013 code of practice and the ServiceNow Information Security Management System (ISMS). ServiceNow has been an ISO 27001 certified organization since 2012 and is also ISO/IEC 27017:2015 and 27018:2014 certified.

ServiceNow provides applications within the Now Platform relating to process and service management. This includes IT service management, based on the globally recognized ITIL process model. ServiceNow as an organization uses

this best practice methodology and its principles to operate and manage its private cloud environment, as well as its customer-facing support model.

Security policy, standards, and procedures

ServiceNow's security program is expressed in its Information Security Management System (ISMS) and its associated security policy and standards. These are reflected in an extensive library of standard operating procedures (SOPs) and other relevant documentation and guidance. SOPs, for example, define the actions that must be carried out in a wide variety of situations in a manner in accordance with overall security policy.

ServiceNow's SOPs include but are not limited to:

- Data handling
- Access entitlements and review process
- Incident management, problem management, and change management
- Configuration management
- Security Incident response
- Risk assessment
- Vendor risk management
- Human resources and information technology onboarding and offboarding
- Secure development procedures

These documents are assessed and updated in the case of significant changes, or at least every two years by a managed program.

Security management

ServiceNow's chief information security officer (CISO), reports to the chief information officer (CIO) and in turn to the CEO. This simple organizational structure provides an executive level of visibility and oversight with respect to security and risk.

The CISO is supported by a number of domain specialist teams. These include security architecture, security engineering, security operations and threat response, application security, and governance, risk and compliance. There are also specific teams for liaising with customers on security matters, shaping employee behavior, creating documentation, and other resources.

The roles of each of these teams and individuals within the teams are clearly defined, and ServiceNow makes good use of information security best practices in its security processes, e.g. segregation of duties and four-eyes requirements.

Risk management

ServiceNow has defined processes and procedures for managing and accessing information system and operational security risks. Regular assessments are performed in order to identify and assess the likelihood and impact relating to risks. These risks can include those regarding unauthorized access, use, disclosure, or disruption to ServiceNow systems and customers. Risks are categorized in accordance with a formally documented procedure. Quarterly security and risk oversight meetings are held to discuss the security and risk items that are relevant to the organization by key internal stakeholders.

ServiceNow manages any risks identified as is required, in a timely and effective manner, to safeguard ServiceNow systems and customer data and ensure minimal disruption to its services.

ServiceNow executive leadership is briefed on a regular basis regarding current and new security risks, as well as on potential threats and related matters that could impact ServiceNow and its customers.

Overall security responsibilities

ServiceNow provides its customers with extensive capabilities to configure their instances to meet their own security policies and requirements. The combination of customer, ServiceNow, and data center responsibilities provides coverage across the entire application and infrastructure stack. The areas of responsibility are shown below.

Responsibility	Area of Responsibility		
	Customer	ServiceNow	Colocation (data center provider)
Data management (classification and retention)	■		
Media disposal and destruction		■	
Backup and restore		■	
Authentication and authorization	■		
Data encryption at rest	■		
Data encryption in flight	■	■	
Encryption key management	■	■	
Security logging and monitoring	■	■	
Vulnerability management	■	■	
Business continuity and disaster recovery		■	
Secure SDLC processes	■	■	
Penetration testing	■	■	
Privacy	■	■	
Compliance: regulatory and legal	■	■	■
Infrastructure management		■	
Security management		■	
Secure configuration of instance	■		
Employee vetting or screening	■	■	■
Environment controls		■	■
Physical security		■	■

Table 1 - Responsibility Map

ServiceNow organizational entitlement reviews

ServiceNow as an organization conducts quarterly entitlement reviews to ensure the appropriate logical and physical rights are assigned to ServiceNow personnel. This includes those responsible for management of its private cloud and physical colocation spaces. Changes to the role of a member of ServiceNow personnel results in the access entitlement being appropriately adjusted without undue delay.

A service catalog of ServiceNow roles and request types is implemented internally. This is used both for new requests and re-assignment of access for existing personnel. This approach mitigates potential incorrect assignment of access, which can occur where access is simply copied from one user to another.

The majority of ServiceNow personnel have no access to any systems hosting customer data, or to customer data in general.

ServiceNow has a dedicated identity and access management (IAM) team with an active IAM entitlement program which requires frequent reassertion of entitlement and comprehensive review.

Privacy and regulatory compliance

Privacy

ServiceNow customers are responsible for determining the collection, storage, usage, sharing, archiving, and destruction of data processed in their ServiceNow instances. As the data controller, ServiceNow's customers are responsible for meeting the requirements of relevant privacy legislation in the jurisdictions in which they operate and from which they collect personal data. ServiceNow fulfills the role of the data processor and complies with any obligations this entails. ServiceNow has no visibility or understanding of the conditions under which the data was collected, if appropriate permission was obtained, or whether it is being used in accordance with those conditions.

ServiceNow's primary responsibility with regard to privacy is to protect the confidentiality of any data its customers entrust to it. Regardless of how a customer has classified the data they choose to store in their instances, ServiceNow implements a single operating and security model for the protection of that data.

Customer data remains the property of that customer at all times. For example, if and when an individual requests information directly from ServiceNow on any data that may be stored about them, or requests to change said data, ServiceNow will always refer that individual to the customer who owns the data.

Regulatory and industry compliance

ServiceNow has a dedicated governance, risk, and compliance (GRC) team responsible for a number of organizationwide compliance efforts, including managing ServiceNow's compliance program. As part of this, they engage across multiple functional areas within ServiceNow, including legal, finance, and procurement.

ServiceNow's legal organization engages both internal and external legal counsel to understand ServiceNow's obligations to existing and new laws and statutory regulations within the jurisdictions in which it operates.

The finance department is responsible for ensuring ServiceNow's compliance with relevant financial regulations, including Sarbanes Oxley (SOX), a requirement for all US public companies.

ServiceNow itself is not subject directly to vertical-specific regulation such as HIPAA, PCI, or NERC-CIP. It does, however, have many customers who are, and through the features in the Now Platform and organizational transparency, it is able to support those regulated customers in meeting their obligations.

In addition, ServiceNow operates a quality management system based on the ISO 9001 standard. The ServiceNow QMS has a dedicated QMS team, quality engineering team, and compliance team to ensure continual improvement of its QMS.

ServiceNow has a comprehensive geographical and industry compliance strategy to support customers. This includes:

ServiceNow certifications/attestations	Geography	Industry or vertical
ISO 27001	International	All
ISO 27017:2015	International	All
ISO 27018	International	All
SSAE 18 SOC 1 Type 2	International	All
SOC 2 Type 2	International	All
FedRAMP JAB High and DoD IL 4 authorization	United States	Federal government/DoD
FDA Quality Management System (based on ISO 9001)	International	Life science
ASD Certified Cloud Service	Australia	Australian federal government
Multi-Tier Cloud Security Standard for Singapore (MTCS) Level 3	Singapore	All
Cloud Computing Compliance Controls Catalog (C5)	Germany	All

Table 2 - ServiceNow Certification/Attestation

Architecture

ServiceNow's architecture provides the template for the ServiceNow private cloud on which the Now Platform is deployed as a subscription service. The cloud is deployed on a highly standardized, redundant, and managed environment. From pre-built racks through to supporting services, such as networking and other logical infrastructure supporting a defense-in-depth model, ServiceNow's cloud exclusively hosts instances of the Now Platform. Each instance is dedicated to a single customer and accessible only by that customer.

ServiceNow operates its cloud out of colocation data centers which provide robust physical and environmental controls. In these locations, ServiceNow's own on-site personnel exclusively provide management, installation, maintenance, and support.

Logical access to the infrastructure hosting the ServiceNow cloud and all hosted customer data is granted only to ServiceNow personnel with the specific requirement to do so. Access where required is provided on a per-role basis, in accordance with specific job functions and a least privilege model, and reviewed regularly.

In accordance with separation-of-duties good practice, ServiceNow personnel with physical access to data centers do not have logical access to data environments, and staff with logical access to data do not have physical access to data centers. The private cloud environment is both physically and logically isolated from ServiceNow's corporate environment, and is also subject to different standards, policies, and governance reflecting its different purposes and dispositions. To manage the private cloud infrastructure, ServiceNow operational personnel only use ServiceNow issued endpoints and a client VPN with two-factor authentication. Access takes place within a virtual sandbox on the endpoint from which employees cannot extract or copy data.

ServiceNow does not outsource any service, operational, or management functions that would provide any third party with access to systems hosting customer data or to customer data itself. ServiceNow limits the infrastructure supporting its cloud's footprint to only those technologies, infrastructure, and components required to support the Now Platform. This approach includes highly restricted networking rule sets regarding ingress and egress requirements and deployment of standardized, hardened systems. These result in a minimal number of necessary services, protocols, and ports being required in provision of the ServiceNow private cloud, thus minimizing attack surfaces.

This exclusive, highly defined and limited environment allows for a number of key benefits:

Automation

Many activities in the ServiceNow infrastructure are conducted entirely using automation with minimal to zero human interaction. For example, where ServiceNow provisions new instances for its customers, this is a completely automated process. Using this approach as an operational pattern creates consistent configurations and expected outcomes, and reduces the potential for, and impact of, human error.

Support, scalability, security

ServiceNow is solely focused on supporting one service: the Now Platform. This is deployed in a private cloud environment dedicated solely to this purpose, and implemented identically in all regions in which ServiceNow operates. The cloud environment supports thousands of identically provisioned ServiceNow instances allowing for significant economies of scale and operational agility. The security risks in a highly homogenous service are often more predictable and easier to manage than in highly diverse environments typical of many enterprises. ServiceNow is focused on only one thing, securing data processed within its infrastructure and instance of the Now Platform.

Control

ServiceNow fully manages the underlying software, services, and supporting infrastructure as well as the software development lifecycle. This allows ServiceNow complete control over all components in its environment and vastly reduces supply chain risks.

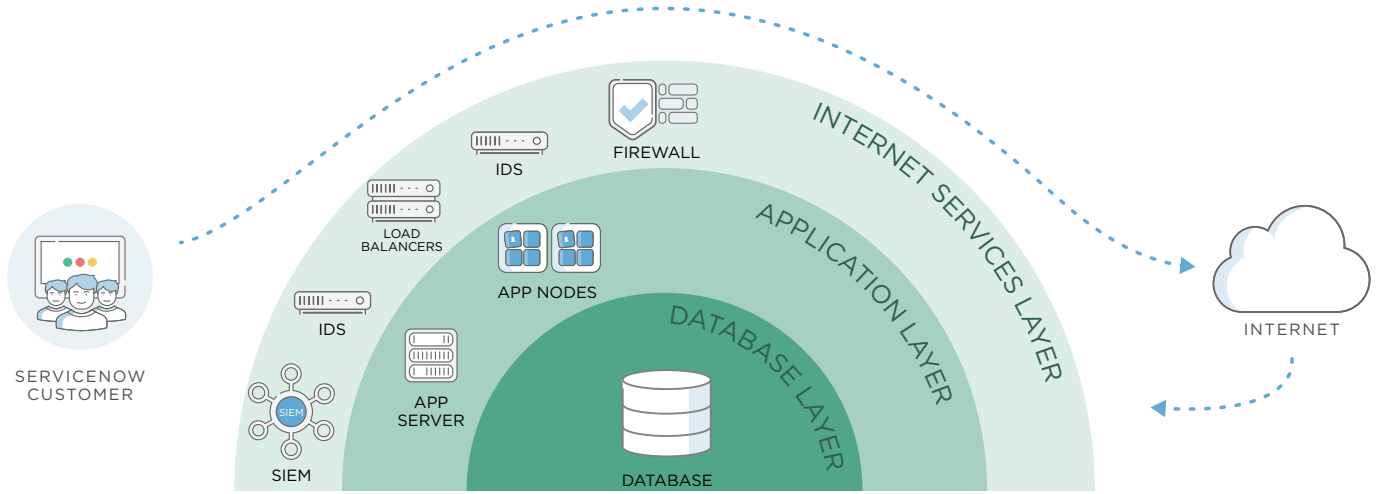


Figure 1 – Three-tier logical architecture model

Logical architecture

The logical architecture of the ServiceNow application is a three-tier model as described below.

Proxy layer (internet services layer)

Customers and web services connect to the ServiceNow private cloud over HTTPS, using TLS for communication to and from a ServiceNow instance. All interactive end-user activities are performed using a standard web browser. There is no requirement for customers to install any client software on any desktop, laptop, tablet, or smart phone in order to access their ServiceNow instances.

This layer forwards requests made from customers' end-users or integrations to the relevant customer instance. This first tier of the application architecture includes network routers, switches, load balancers with integrated network firewalls, and intrusion detection systems. All are deployed at a minimum 2N basis to provide redundancy. Translation of Universal Resource Identifiers (URIs) to ServiceNow internal IP addresses is performed in this tier.

Application layer

In this second tier are application servers in a discrete network segment accessed only via the proxy layer and not directly accessible from the internet. These servers host clustered application nodes for each customer's

ServiceNow instances and are the termination point for all inbound requests made by end-users of those instances. Requests are received by the relevant application nodes and processed by them, including being appropriately escaped or encoded as required, before passing to the relevant database service in the database server tier.

Database layer

The third and final tier consists of database servers, again installed in a discrete, non-internet routable network segment. Requests from end-users or integrations cannot be made directly to the database tier and are only issued from a customer's ServiceNow instance.

Each instance has a single database present on a database server running multiple discrete databases. There is no comingling of any customer data between instances and databases, nor shared multi-tenant databases with data from multiple customers stored therein. For example, if a customer has four instances of ServiceNow, they will have four entirely separate databases and database services, one unique to each instance. These database services may run on different database servers and there is no assumed relationship.

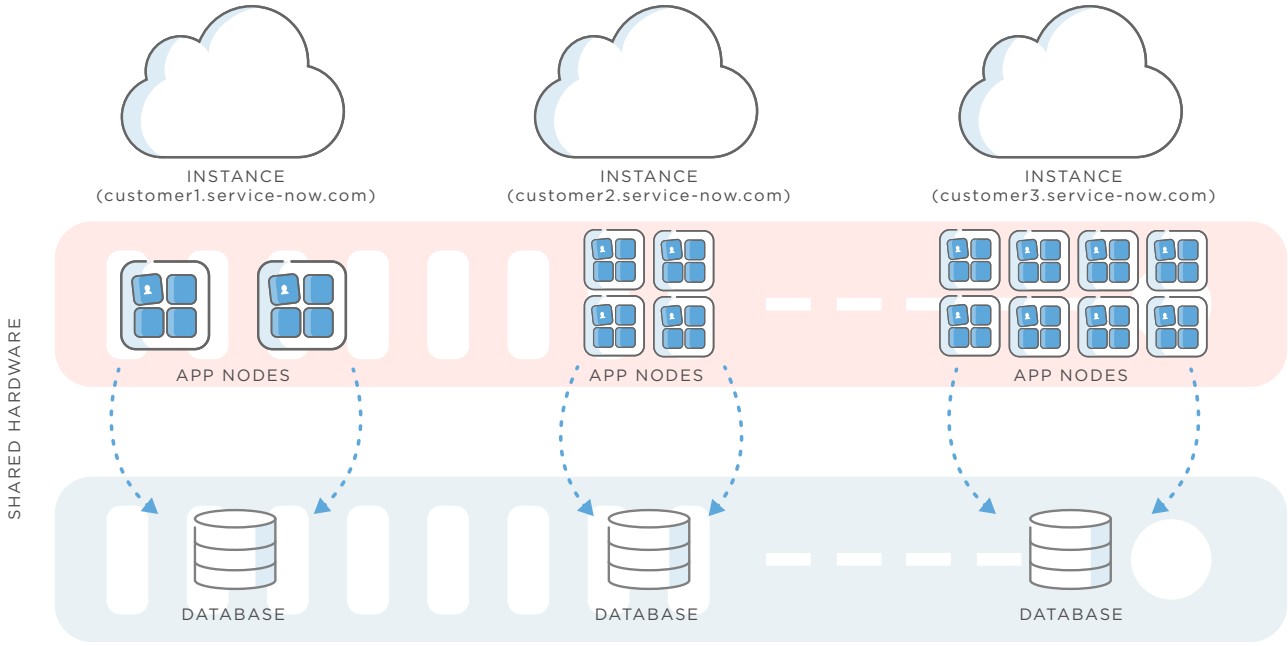


Figure 2: Logically single tenant, physically multi-instance

ServiceNow's customers benefit from multiple layers of robust separation, rather than a single logical control. For example, a number of SaaS provider tenancy models may use tagging of data or records to identify customer data. Access control mechanisms then process these in order to keep customers separated and ensure the data is only visible to the correct customer. Using such techniques has the potential for misalignment of data or records to incorrect owners. Defects, faults, or weaknesses in access control list processing could also potentially lead to data leakage. Because of ServiceNow's defense in depth approach, these two scenarios are extremely unlikely to occur in the ServiceNow multi-instance tenancy model.

A significant benefit of ServiceNow's architecture is that it creates a very distinct boundary between the data of each customer that isn't solely dependent on logical controls. This allows ServiceNow to maintain a highly accurate inventory of the exact location of a specific customer's data at any given time, and customers can access this information directly via the ServiceNow customer support portal. Knowing exactly where all of a customer's hosted data is located also enables ServiceNow to reliably and securely delete that customer's data in its entirety, if required.

The multi-instance tenancy model also facilitates the smooth transfer of customer instances from one application server to another within a single data center, the fail-over of instances from one data center to another within the same region, and the ability to perform upgrades and maintenance on an individual basis without impacting other customers' instances. This enables exceptional instance availability.

Physical architecture

Geographies

ServiceNow hosts its private cloud in colocation spaces within global data centers arranged in high-availability pairs. Currently 11 data center pairs (a total of 21 data centers) exist across four geographic regions. These regions are Asia Pacific Japan (APJ); Europe, Middle East, and Africa (EMEA); North America; and South America.

Figure 3: Data center pairs and support centers

There are also pairs exclusively for qualified US Federal and Swiss banking customers. Meeting regulatory and sovereignty obligations is a significant factor in ServiceNow selecting data center facilities within specific geographic boundaries.

ServiceNow uses top-tier global data center providers. These providers have no logical access to any ServiceNow systems or customer data and solely provide private colocation spaces and environmental resources. Only ServiceNow personnel with a direct responsibility for maintaining colocation spaces are able to physically access data center locations.

Physical

ServiceNow's physical architecture supporting its private cloud is deployed into dedicated, ServiceNow-managed colocation spaces and is implemented globally.

ServiceNow builds and deploys pre-integrated racks (PIRs) for all server and appliance infrastructure and cabling, and rack design standards are rigorously enforced. Within each space, multiple levels of redundancy are established for networking infrastructure, internal links, and related components. At a minimum, this network infrastructure is mirrored, both within a single colocation space and between ServiceNow data center pairs.

Multiple diverse internet connections terminate within these spaces, providing redundant internet access. Servers, appliances, and network devices are multi-homed with redundant components and commodity supplies (i.e. power and network) fed from multiple separate circuits. Where supported, some data centers also feature electrical supply resilience across multiple grid suppliers.

Environmental and physical security

Overview

Data centers procured by ServiceNow are provided by specialist colocation data center operators. These operators provide ServiceNow with a secure and reliable space to operate in. The data centers, as described below, are highly secure facilities with 24x7x365 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility.

Within each data center all ServiceNow equipment is stored in one or more dedicated anonymous ServiceNow cage spaces or private suites.

The details of individual data centers may vary slightly, however, all facilities have similar operating characteristics. In all cases, contractually the data center providers must be either ISO/IEC 27001:2013 accredited and/or conduct regular SSAE18 SOC 2 Type 2 audits.

Physical data center security

Data centers feature a hardened exterior perimeter with defense-in-depth provided by various access control boundaries.

Data center physical boundaries

All data centers have external anti-climb fencing, crash resistant walls, and data center halls that are not directly adjacent to exterior walls. Some locations feature anti-vehicle bollards.

Data centers are divided into zones; these include public, internal, power, environmental, UPS and battery rooms, loading bays, and other zones. The detail of the zones will vary between the data centers, but the principle is applied across them all. Access controls are applied to prevent movement of unauthorized data center staff between each zone in the data center.

The external perimeter of all data centers is lit to allow CCTV systems to provide detailed views, and entrance or exit points are lit. Some data center locations also include motion detection systems on the exterior.

Within the data center physical boundaries, ServiceNow has its own dedicated cages or suites enabling isolation from other data center tenants, including secondary access controls.

Physical intrusion detection

All data centers that ServiceNow operates from have extensive recording CCTV systems internally as well as at the perimeter. Low light cameras and lighting are used to ensure that details such as facial features and number plates can be clearly identified, even at night. Typically, recordings are held for at least 30 days, although the length of recording varies from data center to data center. Only authorized personnel have access to the recording systems, secured with access control lists (ACL), and all access is audited. In addition to CCTV systems, entrances and exits are alarmed both externally for opening and internally for being jammed open. Exterior glass is alarmed for breakage and data center floors are windowless.

Data center providers are contractually obliged to notify ServiceNow in case of security incidents and activities surrounding this obligation are assessed by audit.

Security guards

Appropriately cleared security guards are present at each data center. The security guards manage the exterior gates and reception areas or front desk, respond to alarms, and conduct scheduled and random patrols of the facilities. All security guards are trained in the operational procedures of the data center.

Facility access and personnel access control

The data center operators control access to their facilities via multiple levels of locking mechanisms. While the precise details of the individual data centers vary, all data centers make use of a mixture of lock types, including mechanical, biometric readers, and access card readers with PIN entry. Data center access logs are retained for audit purposes; the retention period varies across providers. Interlocking mantraps are used to control movement between reception areas and corridors that lead to data center floors.

Data center access control systems prevent staff from entering any area in which they are not permitted. Access to the ServiceNow space itself is controlled by ServiceNow using biometric readers, and access card readers with PIN entry. ServiceNow maintains access control lists for its own cages and suites, only permitting limited access for data center personnel where required, i.e. for health and safety purposes.

Physical access audits

ServiceNow maintains and regularly reviews visitor access logs for its cages or suites. Both physical and electronic records of access are made, and ServiceNow requires its data center providers to supply these on a regular interval.

Electrical and environmental controls

ServiceNow's data centers are highly available facilities with redundant electrical and mechanical systems. While not formally accredited, the data centers are designed to operate equivalently to a minimum of the TIA942 Tier 3 standard.

Electrical systems

ServiceNow's data center providers typically offer between 99.999% and 100% power uptime. These levels of reliability are achieved through the use of redundant power providers where available, multiple redundant power distribution paths, generators, UPS systems, multiday fuel suppliers, and multiple independent fuel suppliers.

These data centers can typically operate for at least 24 hours at full electrical load without the requirement of additional fuel. As data center pairs are generally geographically diverse, each data center receives power from a different supplier wherever possible.

Generators and transformers in the data centers are at least N+1 enabled, with distribution networks being either N+1 or 2N. Within the data center ServiceNow will power devices from disparate distribution networks to ensure that loss of electricity supply on one power networks does not affect others. UPS power is provided either by battery or flywheel systems which can sustain systems until generators can be activated.

Environmental controls

The heat, ventilation, and air conditioning (HVAC) systems in the data centers are responsible for maintaining the humidity and temperature within the data center at an optimal level.

Data centers are N+1 redundant for all environmental controls. If humidity or temperature within a part of the data center breaches the parameters set for that zone, alarms will notify building management to resolve the issue.

Fire detection and suppression

All data centers feature fire detection and suppression systems. The specific system implemented may vary between data centers.

Fire detection is provided by very early smoke detection apparatus (VESDA) and heat alarms that are monitored on a 24x7x365 basis.

Fire suppression may be multi-zone, dry-type, double interlock pre-action, and zoned gaseous-based systems or a combination of both. Fire extinguishers are located throughout the facilities and exit signs are prominently displayed.

Human resources security

Upon commencement of the employment process for prospective candidates, ServiceNow undertakes background checks and screening for all roles. Subject to per-country restrictions, these include criminal, employment, financial, citizen status, and government watch lists. Drug testing also takes place in jurisdictions that allow it. Failure to pass these tests will result in either mandatory disqualification from the employment process or a further follow up investigation.

As a condition of accepting employment, ServiceNow personnel are required to sign a non-disclosure agreement, and review and confirm their understanding of the ServiceNow Code of Conduct & Ethics policy along with the Acceptable Use Policy. This confirmation is recorded electronically.

Personnel are also required to undergo annual security and compliance training and fulfillment of training requirements is measured and enforced. The content of the training varies from year to year, as different security topics, risks, threats and requirements are identified. Some examples are listed below:

- Privacy and data protection
- Code of conduct and ethics
- Insider trading and foreign corrupt practices
- Email and instant messaging
- Physical security
- Cloud technologies

During the term of employment, ServiceNow repeats training on an annual basis, maintains contact with its staff through regular notifications, and provides channels for ServiceNow staff to easily report any suspicious activity.

Personnel whose roles may bring them into contact with customer data are also required to undertake additional training.

The lifecycle of a user within ServiceNow is controlled by standard operating procedures for the creation, modification, and deletion of user identities. ServiceNow operates integrated HR, IT, and IAM processes, using ServiceNow's own products, that operate independently for both the corporate environment and the completely separate customer cloud environment.

Access is role based, in accordance with job function and in line with the principle of least privilege. Regular entitlement reviews are conducted to ensure that the processes are working and to remediate any changes or removals that have not been processed appropriately. Employees exiting ServiceNow have all access removed within a maximum period of 24 hours.

Availability

Availability is an essential element of the ServiceNow security program.

Overview

ServiceNow provides a highly available cloud infrastructure through its Advanced High Availability (AHA) architecture.

As ServiceNow's data centers are arranged in pairs, all customer production data is hosted in both data centers simultaneously and kept in sync using asynchronous database replication. Both data centers are active at all times, in a master-master relationship, with data replicated from the active (read-write) data center to the passive (read-only) data center. Each single data center in a pair is implemented so it can support the combined production load of both locations.

Within the regional data center pair there is no concept of a fixed primary location for any customer instance. Although requests are not being actively served from both data centers at the same time, they are both "warm" at all times. As there is no data center affinity mechanism, two instances from the same customer could be operating out of different data centers at the same time.

ServiceNow has two distinct processes relating to ensuring instance availability: transfers and failover.

Transfers

A transfer of an instance is a scheduled event, usually performed for maintenance purposes and always coordinated with a customer. These outages occur within the contracted availability service level agreement ServiceNow commits to with its customers.

Failover

A failover of an instance is an event usually performed where availability for one or more customer instances cannot be maintained. This could be down to a local component failure, or an event such as a major environmental incident or resource outage. In the case of the former, a failover to a system within the same data center will be attempted first. Where a data center-wide outage is identified, all current active production instances in the impacted data center will be failed over to the passive data center location in the pair. In this circumstance, a two-hour recovery time objective (RTO) is targeted by ServiceNow. A maximum one-hour recovery point objective (RPO) is also targeted. Due to the almost real-time replication between data centers, this is usually significantly bested.

Automation technology built on the ServiceNow platform is used to transfer or failover instances when necessary. The mechanism for both processes is very similar. The current passive system is designated active, and vice versa. To complete the process, DNS mappings and instance database configurations are updated accordingly. Redundant DNS providers and DNSSEC are employed to provide robust, resilient name resolution services.

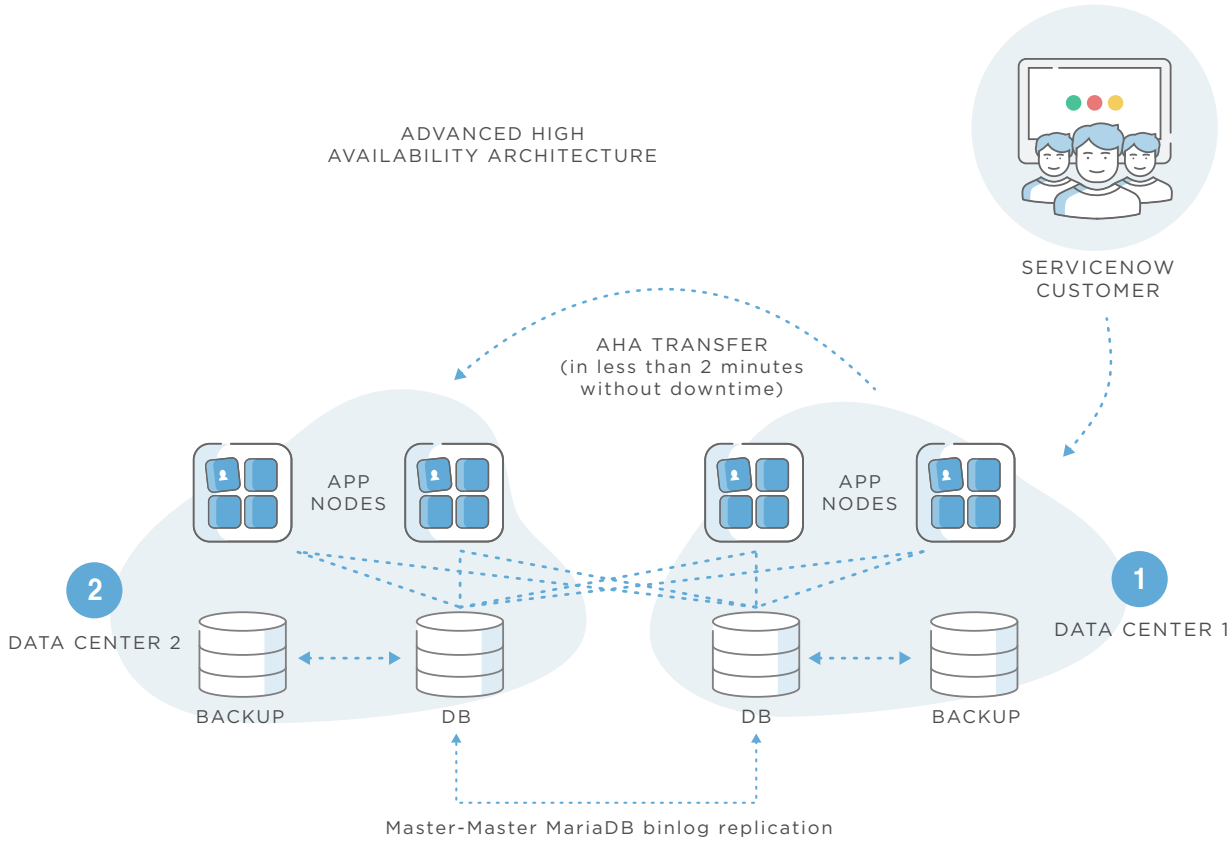


Figure 4: Advanced High Availability Architecture

Data backup

ServiceNow's Advanced High Availability (AHA) architecture is the primary means to restore service in the case of a disruption that could impact availability. However, in certain scenarios it may be desirable to use more traditional data backup and recovery mechanisms. The ServiceNow data backup and recovery system works in parallel to the AHA feature and provides a means to restore previously backed up data.

ServiceNow stores production instance data and their backups in both locations in the customers' elected data center pair. As sub-production instances are not highly available, their data and backups exist only in one location of a data center pair.

The backup cycle consists of four weekly full backups and six daily differential backups which provide 28 days of backups. All backups are written to disk and no tapes or removable media are used. Backups are not sent off-site, but they are made in both data centers within a pair, so benefit from geographic separation. If data is encrypted by the customer in the "live" instance database, then it will also be encrypted in the backups.

ServiceNow restores databases from backups upon a customer's request or in the event of "logical" corruption. This could be, for example, where a customer deletes some data inadvertently. It may also be necessary where a customer's data integration or automation is misconfigured or malfunctions in some way, resulting in data being rendered unusable or inaccessible. In these scenarios, the high availability capability would not assist and hence a restore from backup is the only avenue for recovery. Backups are also used where a system or service failure may in some way impact the integrity of customer data.

Automated testing of backups in progress ensures backup integrity, with any failures reported for remediation within ServiceNow.

The ServiceNow backup architecture is not designed to provide archival records given the maximum 28-day backup retention period; instead it is intended as a recovery process as described previously. Customers may retain data within their instances for as long as they require in accordance with their policy or regulatory requirements. Additionally, there are capabilities within the Now Platform to allow customers to manage logs and regularly export data to external systems as required.

Business continuity and disaster recovery

Overview

ServiceNow is divided into two distinct environments for the purposes of business continuity (BC) and disaster recovery (DR). ServiceNow's corporate IT environment and its cloud data centers are physically and logically isolated from each other. A disaster in ServiceNow's corporate environment could occur with little or no impact on the ability for the data centers within the private cloud to continue to operate.

In both cases, the BC and the DR are supported by a series of tested processes, automations, and supporting documentation, allowing ServiceNow to quickly and effectively take action when availability of its cloud or critical supporting services are affected.

Cloud continuity

Execution

ServiceNow's Information System Contingency Plan (ISCP) covers its cloud data center environments. Its scope includes all customer instances of the Now Platform, as well as those ServiceNow uses internally as an organization to support its business. The ISCP uses ServiceNow's Advanced High Availability architecture as previously described in this document.

Testing and compliance

ServiceNow formally tests its recovery processes on an annual basis and can produce reports relating to this for customer review. ServiceNow also uses the process of transferring instances for maintenance purposes on a daily basis. As a result, ServiceNow is very well practiced at the process of "failing over" or transferring customer instances.

Organizational business continuity

ServiceNow's BC process covers its corporate environment and functional offices. It is therefore a separate process from that used in its cloud environment. The BC Plan (BCP) has been developed in concert with the entire business and includes ongoing Business Impact Assessments (BIA) to understand the impact of the loss of any given systems, services, or physical locations.

ServiceNow infrastructure operations management

As a cloud services provider (CSP), a significant element of ServiceNow's responsibility is to provide and manage the underlying infrastructure on which instances of its Now Platform are deployed. A number of complementary activities and processes are undertaken in managing this environment, all using ServiceNow's own products.

Capacity management

A capacity management team ensures the private cloud is able to support current and reasonably anticipated future load.

Configuration management

Continuous monitoring is undertaken to validate the configurations for each of the system and application components that make up the private cloud.

Change management

ServiceNow adheres to a rigorous change management process that includes mandatory online training for all ServiceNow personnel with an operational role. Change management processes adhere to ITIL v3 principles. ServiceNow processes hundreds of changes a week and thousands of changes each month.

Instance integrations

The Now Platform is based on service-oriented architecture (SOA), in which all data objects can use web services to access bi-directional data-level integration.

Additionally, the platform offers a rich interface for loading external data using import sets. Using this feature, customers can load from various data sources such as HTTPS, FTPS, and SCP using file formats such as XML, CSV, and Microsoft Excel XLS files. Information can also be pulled from a data source using a direct JDBC connection, provided customer network connectivity permits it.

For integration with systems, services, or applications within a customer's network, ServiceNow provides the MID Server component. This capability enables secure integration and collaboration between a customer's own applications and services and their ServiceNow instances. MID Servers may also be combined with import sets for data sources not accessible to a customer's ServiceNow instance.

Information within an instance can be exported and migrated to an external platform using an ODBC Driver, provided by ServiceNow, and forms, lists, and reports on the platform can be accessed directly using a URL, which facilitates integration on the UI level between two or more web applications.

MID Server

The ServiceNow Management, Instrumentation, and Discovery (MID) Server is an optional, free ServiceNow component. It facilitates communication of data between the customer instances and external applications, data sources, and services. MID Servers are used by a customer in conjunction with their instances for enterprise application and service monitoring, integration, Orchestration, and Discovery.

The MID Server is a Java application, provided by ServiceNow to customers via a download link within their instance. It may be installed on a host system of the customer's choosing within their environment. The server can be Windows, Unix, or Linux operating system.

By default, a MID server initiates an outbound session every 15 seconds, to a customer's instance over HTTPS, looking for activities to perform. For example, a ServiceNow Discovery activity to update a customer's configuration management database within their instance. The activity is retrieved, executed, and any output returned to the originating instance. This "pull" approach negates the need to open inbound access through a customer's perimeter or firewalls.

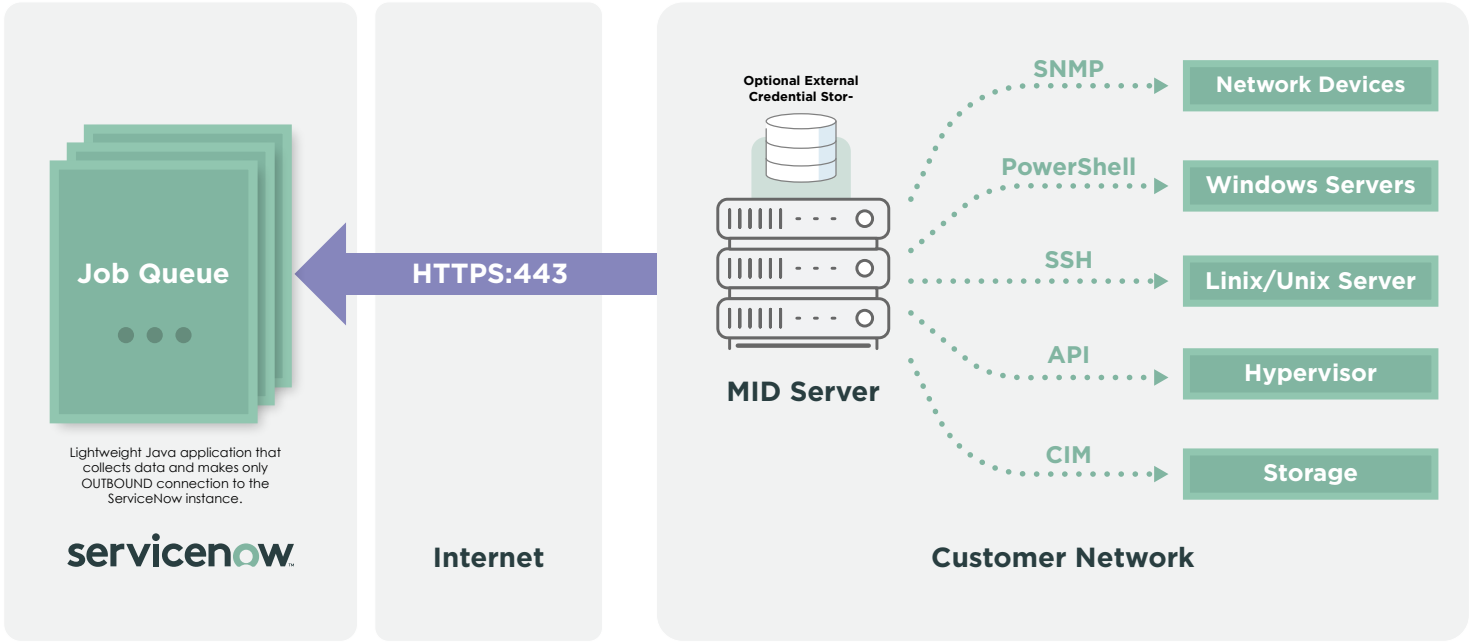


Figure 5: MID Server integration diagram

Web services

ServiceNow supports Web Services using SOAP and REST for integration and therefore all traffic is encrypted using TLS.

Web service security is enforced using the combination of basic authentication challenge/response and system-level access using contextual security. Additionally, there is a set of web service-specific roles that may be granted to the web service user.

Support for WS-Security 1.1 in the form of WSS X.509 Token Profile and WSS Username Token Profile is available for incoming SOAP requests. In this context "incoming" means requests targeting a web services resource in a customer ServiceNow instance.

ServiceNow instances support outbound-only web services mutual authentication by defining a protocol profile for connections that require mutual authentication. Protocol profiles allow you to associate a specific certificate record with a protocol, such as HTTPS. Requests made to an endpoint whose domain is defined in a profile are then mutually authenticated.

Mutual web services authentication is only possible for outbound HTTPS connections, such as SOAP, REST, or direct HTTPS calls. A ServiceNow instance does not support mutual authentication for inbound requests or for outbound requests sent through a MID Server.

Malware protection

The ServiceNow Antivirus Protection feature protects instances against the uploading or downloading of malicious content. File attachments are scanned by dedicated servers in each regional data center to guard against viruses or malware being distributed from the instance.

Instance communication hierarchy

Customers initiate communication to their ServiceNow instance over HTTPS, from any endpoint device with a browser or from a system or application level integration. These requests will both originate within the customer's network.

The instance itself never initiates communication into the customer's network unless a data source or other integration to an accessible resource within the customer environment is configured by a customer.

Activities such as ServiceNow Discovery or Orchestration which can "touch" customer infrastructure are executed only on customer direction. These are via activities they define in their instances, using MID Servers they have deployed. Output from the activities, where produced as part of an activity, is sent back to the relevant instance over HTTPS.

A MID Server will only undertake activities and communicate to systems within the customer network as defined by a customer. A customer can place as many MID Servers in their environment as necessary to support any network topology ranging from a flat to a highly segmented network.

Authentication and authorization

Authentication

A ServiceNow instance provides a customer with a number of authentication options. All can be used simultaneously within a customer's ServiceNow instance, using a multiple authentication model.

Security Assertion Markup Language (SAML) for Single Sign-On (SSO)

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. SAML exchanges security information between an identity provider (a producer of assertions), commonly abbreviated to IdP, and a service provider (a consumer of assertions).

The ServiceNow SAML 2.0 integration enables single sign-on by exchanging XML tokens with an external identity provider (IdP). The identity provider authenticates the user and passes a NameID token to the ServiceNow instance. If the instance finds a user with a matching NameID token (for example, the email address), the instance logs that user in.

The ServiceNow SAML plugin supports SSO-based authentication via a variety of SAML-compliant identity providers. This include Active Directory Federation Services (ADFS) as well as third party identity providers such as Ping, SecureAuth, SailPoint, Okta, or indeed any that are compliant to the SAML 2.0 standard.

Customers who implement their own SAML compliant IdP or opt for a third party service can then also leverage this with other cloud services. When a customer elects to use the SAML plugin, their password and credential policies are governed by their own IdPs.

Lightweight Directory Access Protocol (LDAP)

LDAP authentication lets customers use their own LDAP-compliant directory services such as Active Directory or similar. A directory needs to be accessible to the relevant ServiceNow instance, as often these are located behind a firewall or other perimeter control.

"Meta" directories including Lightweight Directory Services can alternatively be utilized to permit safe access to a customer's LDAP directory from a DMZ or similar. Secure LDAP (LDAPS) is supported.

With an LDAP integration, the authentication path commences with an end-user providing their username and password to the customer's ServiceNow instance. These credentials are then used by that instance to perform a simple bind against the customer's target directory service for that user. If successful, the user will be authenticated to the relevant ServiceNow instance. Multiple Directory Service sources may be configured.

As part of the LDAP integration, passwords are not stored nor transferred back to the customer's ServiceNow instance.

Customers who elect to use their own LDAP directories have their password and credential policies governed by the policies set within these.

Built-in "native" authentication

In the case of native authentication, passwords as well as other user attributes are managed solely by the customer within their instances of ServiceNow. This is the only authentication method where both the username and password are stored within a customer's ServiceNow instance.

When using native ServiceNow authentication, properties such as the length, complexity, rotation, and uniqueness of passwords are customizable by a customer.

In this authentication option, passwords are stored as a 1-way SHA-256 hash, with an appropriate salt value.

OAuth 2.0

OAuth 2.0 allows customers to access instance resources through external clients by obtaining a token rather than by entering login credentials with each resource request. OAuth 2.0 is implemented in the Now Platform for the following scenarios:

Auth external client scenario	A customer's instance provides an endpoint for third-party clients to pull data from the instance.
Auth provider scenario	A customer's instance pulls data from a third-party provider.

Authorization

Customers have full control of entitlements granted to each of their users in a ServiceNow instance.

A ServiceNow instance includes a built-in role based access control (RBAC) mechanism providing user, group, and role objects. These can be used by a customer to assign access to applications and data within their instances. Customers can add additional users, groups, and roles to those already defined.

Access control lists (ACLs) are used in conjunction with RBAC to control access to entire tables, records or fields. A number of default ACLs will exist in an "out-of-the-box" ServiceNow instance. Customers can add to those per their own requirement.

ACLs comprise individual entitlements which include create, read, write, and delete. In addition, access can be further controlled on a contextual basis, depending on individual attributes of the object being accessed. These attributes could include the state of a specific kind of record, the value of a field, or even the day, date, or geographic location of the end users. The attributes available also vary, depending on the type of object being secured.

Additionally, and as described previously, integration with a customer's own directory services is also possible. This then enables a customer to leverage existing users and groups in those directory services to manage users and access within their ServiceNow instances.

User identity synchronization

A ServiceNow instance requires every user to exist as an identity within its database, regardless of authentication mechanism. This identity is necessary to support a wide variety of capabilities within the product, including for role-based access purposes.

To facilitate this requirement, ServiceNow instances support both automated and manual creation of user identities. This includes synchronization of users, their group memberships, and those group objects themselves. Customers may incorporate as few or as many user attributes as they deem necessary. User object passwords cannot be synchronized.

User and group objects can be uploaded into a ServiceNow instance through the use of import sets. These can utilize various types of data source for user and group objects intended for use with a ServiceNow instance. This process is commonly used for initial user uploads to populate the ServiceNow user and group tables in a customer's instance, but can also be used for ongoing synchronization of these. Customers can also simply import a flat file exported from the chosen authoritative identity source. If a user exists in a customer's IdP but are not in their ServiceNow instance, SAML user provisioning can automatically create the users in the instance.

A common approach to maintaining identity data is for a customer to use their own LDAP directory. This would be configured in an import set as a data source for user and group objects. This then allows synchronizing the information in a customer's ServiceNow instances with that in their own directory service. Customers specify the interval or regularity of synchronization per their own requirements. This would usually be daily as a recommended minimum.

Customers may also leverage the ServiceNow MID server component for LDAP synchronization. This component negates the need for a customer to allow their ServiceNow instances through their perimeter and firewall in order to access their internal directory servers. Instead, the customer installs the MID server inside their internal network from where it can access the directory server and return a payload of users or groups and their attributes to the customer's instance. These would then be automatically imported or updated in the target user or group tables within the instance.

Customer access management

ServiceNow customers are responsible for the management of user identities within their instances. This includes the creation of individual identities for each of their users, both internal and external, the methods used to authenticate those users, password policies (for built-in authentication), and the entitlements and access levels granted to those users.

High Security Settings

A High Security Settings plugin provides advanced security options for instances of ServiceNow. This plugin is enabled in all new instances and cannot be disabled. The plugin enforces the default deny access mode, enables access control rules, and provides elevated access functionality and security related roles for a customer's administrators.

The settings also include a number of out-of-the-box security related properties. Customers may access and enable these from a single page in their instances. For example, restrictions can be set on the nature and type of attachments that can be uploaded into the instance, how those attachments behave when downloaded, and other hardening attributes. ServiceNow adds new security properties in each release. Advice and guidance can be found in ServiceNow's Security Best Practice Guide on the HI Service Portal and the Instance Hardening Settings on ServiceNow Docs.

Security logging and monitoring

For the purposes of customer security, ServiceNow collects and retains logs and events relevant to its entire cloud infrastructure. It also collects information on requests made to instances of the Now Platform in order to detect potentially malicious actions or activities in relation to its service. ServiceNow uses such log and event management in conjunction with its ongoing operational security and incident management processes. This information is not available to customers within their ServiceNow instances.

Events that occur within a customer instance are accessible to that customer in their instance logs. Events that happen to a customer instance are captured in ServiceNow's infrastructure logs.

ServiceNow instances

A ServiceNow instance generates detailed log and audit information regarding activities which take place within it. ServiceNow's default application logging capabilities include verbose transaction, client, event, email, and system logs.

Log information is stored, like all customer data, within tables in a customer's instance. As with any customer data, ServiceNow does not access this data in any way during normal provision of its service. Customers manage and monitor the various logs in their instances as they would any other information within an instance.

Log and audit data is protected by access control rules in the same manner as all other customer data. Access to log information is usually limited to administrative roles only.

Logs and events can also be forwarded to a customer's own logging system or SIEM environment. This can be achieved using the syslog probe, utilizing the MID server, or by making direct web service calls to the various log tables. Customers may also simply download or export log table entries or list views containing items of interest. These techniques allow for log and audit events to be stored within a customer's environment and retained according to their specific requirements.

Transaction logs represent every click, view, and system event that occurs in an instance. As a result, they will grow very quickly. These logs include a level of detail useful for customers when troubleshooting issues, as well as providing detailed intelligence on behaviors within an instance.

Event logs include the creation of an incident, or deletion of problem, or any one of a number of standard, pre-configured events. They may also be extended to contain customer defined events.

A number of security related events are also available in the event log. These include those recording successful login, failed login, security privilege escalation, and viewing of tables or records.

As well as reviewing logs manually, workflows or actions can execute when a specific event or log entry is detected or a metric is reached, such as failed logins per minute or access to sensitive administrative roles. These actions could be to issue a notification via email, raise an incident to investigate the matter, or even perform an activity against an application, system, or device within a customer's network.

Audit history is the final aspect of activity logging and recording. This feature relates to recording all activities in respect to customer data and customizations within their instances.

For any particular table or field, audit history may be turned on (or off). The audit history feature then maintains a record of who made any change, when the change took place, and what was changed.

A number of tables are audit-enabled by default and audit history is perpetual for the lifetime of that record; in other words, it is retained indefinitely in the instance.

ServiceNow infrastructure

A key component of any security program is to maintain detective controls. These are required to monitor for potential threat actors and intrusion attempts into the ServiceNow cloud and corporate environments.

ServiceNow has a formal, documented security incident response policy, process, and workflow. Its incident response process includes event discovery, triage, escalation, notification (including customer notification), remediation, and post-mortem review. If a customer environment or data is impacted, the customer will be notified via their normal support contacts without undue delay. Contractual commitments can be viewed by accessing the DPA here: http://www.servicenow.com/schedules.html

ServiceNow has deployed a redundant intrusion detection system (IDS) monitoring network traffic as it transits into its cloud network. This feeds ServiceNow's security information and event management (SIEM) systems. ServiceNow maintains separate SIEM systems for its corporate and cloud environments, with further logical separation for SIEMs

tasked with network, device, and security events. Alerts and notifications are generated by the SIEM systems in accordance with pre-defined triggers and metrics that are updated constantly. These are reviewed by a 24x7x365 security operations capability with global coverage.

ServiceNow tunes and adjusts monitoring to meet the specific characteristics of ServiceNow instances. For example, approved customer penetration tests need to be differentiated from illegitimate or malicious penetration attempts. The SIEM helps support the processes in place that enable ServiceNow security operations to undertake such determinations reliably and promptly.

Events, alerts, and relevant logs are also fed from other systems, including all servers, network devices, and ancillary systems into the SIEM. This allows ServiceNow to build and maintain a comprehensive manifest of the activities that are occurring in its environment on a day-to-day basis. Security alerts, events, multiple threat feeds, and other relevant information are stored and aggregated into an internal ServiceNow instance used for their ongoing management.

ServiceNow is responsible for managing its SIEM environment and securing the events within it. Separate teams are responsible for the configuration and maintenance of the logging infrastructure and the data it generates, to ensure good separation of duties. Network traffic log events are retained for a minimum of 90 days, with infrastructure events being kept for one year.

ServiceNow security operations team is also responsible for completing daily checklists across a range of security domains, including privileged account usage, IDS alerts, file integrity monitoring (FIM), and database access. The daily checklists and captured events are managed through a ServiceNow instance. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.

Software development: Security by design

Overview

As a leading SaaS provider, it is essential that security is an integral part of our software development efforts.

ServiceNow uses an agile development process that includes independent validation steps run by a separate quality team. A requirement of this process is to produce a validation report which includes security as a required signatory to the release process. This allows effective prioritization of remediation efforts and provides security feature requests into the application.

Developers and other relevant personnel are trained on an ongoing basis through a variety of methods, including classroom-based training covering web application security. This includes, but is not limited to that from organizations such as the Open Web Application Security Project (OWASP).

Application security testing

ServiceNow's penetration testing regime is a vital component of its development practices and as a result the penetration testing program is wide-ranging and extensive.

Testing during development

Application security testing occurs throughout the development phase. This is undertaken using a variety of approaches. During development, code for the ServiceNow main branch is subject to continuous ongoing testing and review within ServiceNow using a variety of methods. Commercial and in-house automated toolsets, including static application security testing, are used as well as manual testing and peer code reviews. These efforts are all specifically in relation to security and detection of vulnerabilities at the application code level.

Dynamic application security testing (DAST) is performed on all currently supported versions of the Now Platform. Appropriate patches and hotfixes are included in the scope of this testing.ServiceNow manages and maintains commercially available and custom toolsets for testing. These are continually reviewed and changes are made as necessary, as the Now Platform evolves.

Any validated security issue found is also checked for and if necessary remediated in all earlier supported versions. This remediation is provided either in the next patch for that release, or as a hotfix, subject to criticality.

Application penetration testing

After internal testing comes a phase of external application penetration testing. The intention of this process is to

provide independent review and transparency around ServiceNow's secure development practices. A third-party organization is given an extended period of time and access to the resources necessary to review and test the next release of the Now Platform before it is made available to customers.

On completion of a first round of testing, any confirmed issues are entered into the ServiceNow problem resolution process, prioritized, and categorized. Those whose impact and criticality meet pre-defined ServiceNow criteria are remediated prior to any re-testing.

Once the remediation completes, a second round of testing is conducted, again by the same third-party organization. This is in order to confirm the provided remediation or mitigation functions as expected.

Results of the third-party testing are consolidated into an executive summary report which can be shared with existing customers using that version once released.

Customer application penetration testing

Another significant aspect of ServiceNow's application penetration testing regime is tests performed by its customers.

Through a documented process on the HI customer support portal, existing customers are permitted to perform an annual application penetration test. Scheduling of testing must be pre-approved and conducted at a date and time agreed with ServiceNow. This is necessary to allow ServiceNow to continue to conduct its monitoring activities and be able to differentiate potential attacks from authorized customer testing.

Customers must upgrade their instances to the latest release and patch version prior to any testing taking place. They must also implement ServiceNow's hardening guide before conducting any testing. Testing without these pre-requisites will result in false positive identification of previously identified issues. As a requirement for the process, customers are required to share their results with ServiceNow.

Confirmed customer findings help contribute to the collective security of the ServiceNow environment and enable a continuously improving security posture, and the customer penetration testing scheme supports a significant number of tests annually across the customer base. Confirmed vulnerabilities discovered by this process are remediated in accordance with ServiceNow's vulnerability management criteria.

The release notes on the ServiceNow docs site for each major version, patch, and hotfix include information regarding what has been remediated in each release, including those that are security-related.

Application security teams

ServiceNow has dedicated teams of security engineers who are part of the ServiceNow security office and are deeply integrated into the overall software development program.

The teams perform a number of functions, including but not limited to:

- Managing the various internal and external testing programs
- Performing assessments of internal ServiceNow services and organization instances used for running its business
- Performing architectural reviews in respect to new features security features
- Curating educational security materials, including those for customers

ServiceNow Security Operations Management

Infrastructure vulnerability management

ServiceNow maintains an ongoing infrastructure vulnerability program using third-party commercial and in-house tools to identify vulnerabilities in the ServiceNow perimeter and for all cloud and corporate systems.

Identified vulnerabilities feed into the overarching vulnerability monitoring and remediation program. As necessary, patching of affected systems, services, or applications is undertaken promptly, in accordance with ServiceNow criteria and processes.

Infrastructure vulnerability scans occur daily for public facing infrastructure, on an unauthenticated basis. Weekly scans are performed on an authenticated basis for internal, non-Internet routable infrastructure.

Operating system security

ServiceNow builds and maintains standard network device, appliance, and operating system build configurations. New devices and servers are deployed with automatic configurations relating to their function.

Controls relating to the monitoring of sensitive operating system files and restrictions on lateral movement across data centers are also in place. Anti-malware measures with regular updates are made to all servers within the private cloud, as well as all ServiceNow corporate IT systems and endpoints.

Infrastructure and application security services

As described previously in this document, ServiceNow has intrusion detection capabilities within its private cloud. In addition, all relevant services and system components send security logs and events to a SIEM for security monitoring and alerting.

Distributed denial of service (DDoS)

ServiceNow employs a significant range of detective controls to monitor and prevent potential DDoS attacks from impacting the ServiceNow private cloud environment. This includes the implementation of in-house DDoS protection mechanisms, provision of significant Internet bandwidth connectivity, and the use of third party services to mitigate against such attacks.

Vulnerability management

At a high level, vulnerability management at ServiceNow falls into two primary domains: Now Platform and cloud infrastructure.

Now Platform

ServiceNow generally produces two releases of the Now Platform annually. In addition, patches and hotfixes are produced throughout the supported lifetime of a major release and rolled into the codebase for inclusion in the next version.

To ensure you are benefiting from the most current security, performance and functional fixes, ServiceNow will apply patches to your instance(s) on a continual basis as part of the new ServiceNow Patching Program. Each quarter, one full patch and two security patches will be automatically scheduled to update your instance(s) to the minimum required patch version.

An instance of ServiceNow may continue to be used while a major release upgrade, patch, or hotfix installation takes place. Patch application leverages the Advanced High Availability capability and results in minimal impact to service where any update is applied.

ServiceNow requires customers to remain on a supported release of the Now Platform and will actively engage with customers' risk and security personnel to highlight the risks of non-compliance.

Cloud infrastructure

Findings reported from the continuous scanning of its infrastructure by ServiceNow's vulnerability management tools are automatically logged within an internal ServiceNow instance. These are first reviewed by ServiceNow personnel to determine that the appropriate level of priority is assigned, taking into factors such as relevant mitigating controls and exposure. Those issues identified at the highest risk classification level will be targeted for remediation as quickly as possible.

ServiceNow's Infrastructure stack is customized at each

layer to specifically support the Now platform. Publicly identified vulnerabilities in common software platforms (e.g. CVEs) may not necessarily present a risk within the context of the Now Platform. This can be due to factors such as absence of the affected software or component in the ServiceNow environment, or its limited or complete inability to access the Internet.

ServiceNow does not condone any attempts to actively audit our infrastructure. However, we recognize that vulnerabilities in our systems, products, or network infrastructure are occasionally discovered incidentally. If you discover a vulnerability, please report it to us in a responsible manner per the guidelines located here.

Alternate techniques are also used to address vulnerabilities where no clear remediation, i.e. a vendor patch, is available. So-called "virtual" patching is implemented in such circumstances as necessary.

Once it is determined that a patch needs to be deployed, this effort enters the change management process. In this process the assets, risk, and potential impact to the relevant environment are identified along with the testing required, back-out plan, and timeline for deployment.

ServiceNow again leverages the Advanced High Availability architecture to transfer customers' production instances between data centers when performing infrastructure maintenance such as patching, thereby minimizing the impact to availability.

Information lifecycle and data management

Information classification

ServiceNow applies a single data classification to all customer data it hosts. ServiceNow does not inspect or monitor its customers' data and has no ability to understand how any data may have been classified by individual customers. For ServiceNow, the overriding requirement towards customer data is that it remains hosted solely in the private cloud and is treated and handled in accordance with its policies for all customer data.

Customers remain the data owner and data controller for all data they place into their ServiceNow instance, and should apply access controls to restrict access to data within their instances based on their own requirements and needs, in accordance with their data classification policies.

Data retention

Customers decide what information is to be stored, how it is to be used, and how long it is retained. ServiceNow does not delete or modify customer data and only processes data in accordance with its contractual obligations and the customer's configuration of their instance(s).

For data deleted by a customer from their instance, the deletion in terms of regular access will take place immediately, and will take 28 days to be cycled out of a backup of that instance.

Media disposal

ServiceNow hosts its customer data only on solid-state (SSD) or mechanical disks within its data center colocation spaces. No tapes or other forms of removable media are used in providing the service, including for backups, which are written to disk. Functioning mechanical storage devices which are retired at end of-life, or for re-assignment to new customers, are logically shredded using a process based on guidance from NIST. SSD drives are securely erased with processes utilizing appropriate tools provided by the relevant SSD hardware vendor.

All failed storage devices, both mechanical and solid state, are securely retained within the datacenter colocation space in which they were used - regardless of whether they contained customer data or not. They are then physically shredded in a destruction process managed and performed by ServiceNow and tracked using a change management process.

Data return and destruction

Throughout the lifetime of the subscription, data can be directly exported using features available in a ServiceNow instance. This can be via the UI interface, through integrations, or by using optional ServiceNow components such as the free ODBC connector or MID Server.

Upon contract expiration or exit, or where requested, ServiceNow will supply a customer's data in an SQL dump format. Exiting customers have 45 days to request their data to be returned, after which all hosted and backed-up data is automatically deleted and overwritten.

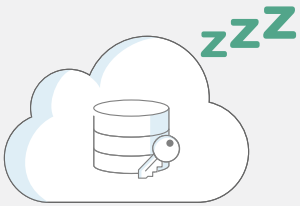
Encryption

ServiceNow provides all enterprise customers with encryption for data in transit. Optional features for encryption of data at rest are also available and may be applied or layered as needed.

This section summarizes encryption capabilities at a high level; a detailed ServiceNow Encryption Technical Summary white paper that describes these features in more detail is also available.

Encryption in transit

ServiceNow customers access their instances over the internet using Transport Layer Security (TLS) encryption using AES with 128-bit or 256-bit cipher suites. Negotiated ciphers are subject to customer browser versions and may be influenced by customer internet proxy infrastructure. Customers can force specific cipher suites via their own browsers or proxies if desired. All end-user access to a ServiceNow instance attempted over HTTP are redirected to HTTPS.



Encryption at rest

Now Platform Encryption

ServiceNow instances provide customers with optional mechanisms to implement encryption for data at rest.

Column encryption

Fields and attachments: A built-in feature which provides symmetric data encryption on a per field basis. Customers may select AES128, AES256 or 3-TDEA (3DES) as encryption algorithms and are required to provide suitable encryption keys. Customer keys are re-encrypted (wrapped) with a secondary key to mitigate compromise of customer encrypted data. Data stored in fields encrypted with this feature cannot be searched or reported on. Fields in the instance with a “system” flag or those used in customer workflows and automation cannot be encrypted.

Edge encryption

Fields and attachments: An additional cost feature which performs data encryption inside a customer’s network using encryption keys stored and managed only within that customer’s network. All encryption takes place inside a customer’s network via a proxy application that functions as a cloud access security broker (CASB). When utilizing this feature, unencrypted target data is never stored in a customer’s ServiceNow instance. Edge encryption also includes tokenization and substitution of data that matches standard data structures such as credit card or social security numbers.

Further information on both of these encryption features is detailed in:

https://www.servicenow.com/content/dam/servicenow/documents/whitepapers/wp-data-encryption-with-servicenow.pdf.

Infrastructure at-rest data encryption

Database encryption

Database encryption encrypts all customer data at rest in the database with no impact to functionality. It utilizes the native capabilities of the database engine to encrypt data as it is written to the database and decrypt as it is read from the database using AES256 encryption. This technology, often called “tablespace encryption” or “transparent data encryption”, is fully transparent to the customer and to the application. ServiceNow applications as well as custom applications can operate seamlessly without any changes necessary because the application always has access to the data it needs in the clear. When using database encryption all data is encrypted, including attachments, logs, and backups.

Full disk encryption

An additional cost feature which provides encryption for data at-rest only, via self-encrypting hard drives. AES256 bit encryption is implemented in these devices and in the key storage appliances that support them. This capability also requires the purchase of dedicated ServiceNow hardware at further additional cost. It is solely intended to mitigate data exposure through the loss or theft of storage devices used for customer data.

Wherever possible, ServiceNow leverages FIPS 140-2 certified technologies in its federal environment.

Integration encryption

Encryption can be applied to integrations such as LDAP and Web Services. LDAPS connections require customers to provide certificates for their specific LDAP servers. Certificates may also be stored within an instance for use in signing of instance-bound web service requests. ServiceNow instances also support certificate-based mutual web services security authentication with external endpoints. FTPS and SCP can be used as file transfer methods to securely transfer data to their ServiceNow instances. Customers may also choose to use clear text protocols such as FTP or HTTP if desired.

Email in-transit encryption

Customers commonly configure ServiceNow instances to generate emails in relation to service management tasks, for example, to request approval for a change or notify a user of the status of a service request. ServiceNow instances provide additional confidentiality in this respect by supporting opportunistic TLS for email sent or received. This feature is subject to a customer’s email infrastructure being capable of establishing an encrypted handshake with the ServiceNow cloud environment.

Key management

Encryption keys provided by customers for use with the column encryption feature are backed up within the database for the customer instance where they are used. Customers should back up column encryption keys prior to applying them to their instances.

As previously stated for column encryption, customer keys are re-encrypted using a wrapper key, commonly referred to as a key-encrypting key, which is stored and managed from a key management appliance.

Encryption keys for the Edge Encryption feature are managed entirely within a customer’s network boundary. Encryption keys for database encryption are managed by ServiceNow using a three-level key hierarchy. The first two keys are customer specific and are created by the database engine, while the third key is instance specific.

Encryption keys used within ServiceNow's cloud infrastructure are managed by ServiceNow. Organizational key management consists of a number of components. Keys are stored in redundant secure key storage appliances. Dual controls are required for essential functions such as generating, deleting, or exporting keys. Key custodian forms are required as part of the generation of new keys. Cryptographic management is undertaken by a specific team within the security group, including appliances used to store the per customer instance wrapper key.

Standard operating procedures are used for the procurement, generation, and configuration of key appliances. Work instructions are used for the configuration and backup of key management appliances with logs from these forwarded to the ServiceNow internal SIEM infrastructure.

Mobile application security

The native ServiceNow mobile applications for iOS and Android enable instances to be accessed from mobile devices. These apps use the same robust authentication mechanisms previously outlined. Once authenticated, mobile users are subject to the same access controls as other users.

Mobile application security controls

The apps benefit from mobile-specific security controls such as restricting clipboard operations, requiring a PIN for access, disabling attachments, and obscuring the app screen when in the background.

Data security

All data in transit is protected with TLS, and application preference information stored on-device is encrypted. By default, no data from an instance is stored on the mobile device, though that is configurable.

Application distribution

ServiceNow's mobile applications can be distributed with common Enterprise Mobility Management (EMM) or Mobile Device Management (MDM) platforms.

Summary

The ServiceNow environment supporting the Now Platform is a dedicated cloud, fully owned and operated by ServiceNow. This infrastructure supports a multi-instance, logically single tenant architecture that enables isolation of customers from each other and provides real-time visibility of customer data location.

Key security benefits are provided through the application of extensive automation, implementation of a consistent global infrastructures, and standardized operational processes.

Customers can augment their instances with integrations to their own applications, services, and infrastructure as well as adopt built-in platform security features such as data encryption and network access control.

Finally, ServiceNow believes its customers are well-served by its application of relevant, measurable, and industry recognized information security frameworks. These include ISO/IEC 27001:2013 and and ISO/IEC 27017:2015 and 27018:2014, as well as accreditation with regional standards and regulations.

Transparent disclosure is an additional element of assurance available to all customers. This includes, but is not limited to, provision of the SSAE18 audit reports and ISO certificates.

For further information on ServiceNow, please visit www.servicenow.com or contact your account representative.

FEDRAMP GOVERNMENT USE ADDENDUM FOR NONFEDERAL ENTITIES

This Government Use Addendum ("**Addendum**") is made as of the Effective Date between the customer entity provided below ("**USG Customer**") and ServiceNow, Inc. ("**ServiceNow**"). This Addendum is added to the terms of the Master Ordering Agreement currently effective between the parties (the "**Agreement**"). Capitalized terms not defined herein shall have the meaning ascribed to them in the Agreement.

EACH ACTING UNDER DUE AND PROPER AUTHORITY, THE PARTIES EXECUTE THIS AGREEMENT AS OF THE EFFECTIVE DATE.

USG Customer: _____	**ServiceNow, Inc.**
By: _____ *(signature)*	By: _____ *(signature)*
Name: _____ *(printed)*	Name: _____ *(printed)*
Title: _____	Title: _____
Signature Date: _____	Effective Date: _____
Address for Notice:	**Address for Notice**: 2225 Lawson Lane. Santa Clara, CA 95054, USA Attn: Legal Department Notices Copy to: legalnotices@servicenow.com

The Federal Information Security Management Act of 2002 and the Federal Information Security Modernization Act 2014 (collectively "**FISMA**") requires each government agency to develop, document, and implement programs to provide information security for the information and information systems that support the operations and assets of the agency. To address the needs of United States ("US") Federal, State, Local and Tribal Governments along with regulated organizations that have a requirement to meet US Federal Government security standards (each a "**USG Customer**"), ServiceNow offers the ServiceNow Government Community Cloud ("GCC") service (the "**Government Cloud**"). Any USG Customer organization other than US Federal Government entities or instrumentalities must demonstrate they have a requirement to meet US Federal Government security standards by contractually agreeing to the terms in this Addendum.

A Federal Risk Authorization Management Program ("**FedRAMP**") accredited Third Party Assessment Organization performed a security control assessment of the Government Cloud at the FIPS 199 High impact level in accordance with OMB Circular A-130, NIST Special Publication (SP) 800-37, and the FedRAMP Security Authorization Process. After review of the Authorization to Operate ("**ATO**") package, the FedRAMP Joint Authorization Board ("**JAB**") deemed the risk to government operations, data, and assets resulting from the operation of the information system to be acceptable, and accordingly issued ServiceNow an ATO for the Government Cloud for the benefit of USG Customers (the "**Security Authorization**"). The conditions for maintaining the Security Authorization to operate the Government Cloud require the physical and logical restriction of the storage of data to hardware dedicated exclusively to USG Customers. Further, Administrative Access to the Government Cloud must be restricted to individuals that are US Citizens that have undergone a suitability check by USG Customer ("**Approved Personnel**"), and each USG Customer accessing or using the Government Cloud must comply with this Addendum. For purposes of this Addendum, Administrative Access is defined as USG Customer's primary administrator(s) role within a ServiceNow instance, that has access to all system features, functions, and data, regardless of security constraints. Each USG Customer is responsible for performing its own risk analysis and monitoring the Customer Data that is processed by the Government Cloud. Any USG Customer may request copies of the information package describing the Security Authorization from ServiceNow or the FedRAMP Program Management Office (https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2017/02/FedRAMP-Package-Request-Form_V5_03012017.pdf), which shall be treated as Confidential Information under the Agreement or disclosed pursuant to a non-disclosure agreement between ServiceNow and the USG Customer, as applicable.

1. USG CUSTOMER RESTRICTIONS. USG Customer shall: (a) restrict Administrative Access to the Government Cloud exclusively to Approved Personnel; (b) use the Government Cloud to only process its own Customer Data; (c) use a naming convention that conspicuously identifies the Government Cloud Subscription Service accessible to USG Customer to the exclusion of any other Subscription Service (e.g., *agencytest*, *agencyprod*, and *partner-agencytest*), or any naming convention recommended by ServiceNow; (d) operate instances in the Government Cloud that are discrete and separate from any and all instances of the Subscription Service accessible to USG Customer that are not included in the Government Cloud; (e) promptly notify ServiceNow by email to legalnotices@servicenow.com in the event that any of the terms of this Addendum are breached; (f) provide ServiceNow the contact information for a Chief Information Security Officer, or equivalent, designated by the USG Customer; (g) have and maintain an internal

acceptable use policy and a plan to communicate such policy to its employees, contractors and agents as needed to ensure compliance; and (h) provide evidence of USG Customer's compliance with this Addendum upon ServiceNow's reasonable written request.

2. ASSISTANCE WITH COMPLIANCE. USG Customer acknowledges that ServiceNow may only retain the Security Authorization if each USG Customer successfully complies with the terms of this Addendum. USG Customer represents and warrants that it will comply with the terms of this Addendum, and has a requirement to comply with one or more of the below laws, regulations, rules, or data standards, as applicable, while operating in the Government Cloud.

- FISMA
- FedRAMP (up to FedRAMP High)
- Department of Defense Security Requirements Guide (up to DoD Impact Level 4)
- NIST SP 800-53
- OMB Circular A-130
- NIST SP 800-37
- International Traffic in Arms (ITAR)
- Covered Defense Information
- Controlled Unclassified Information (CUI)
- Department of Defense (DoD) Unclassified Controlled Nuclear Information (UCNI)
- Department of Energy (DoE) UCNI
- Criminal Justice Information (CJI)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Requirements imposed on organizations from U.S. Federal government agencies (i.e., Department of Homeland Security, Department of the Treasury, Office of the Comptroller of the Currency, Centers for Medicare and Medicaid Services, etc.)

The parties agree that either party's failure to comply with the terms of this Addendum constitutes a material breach of the Agreement.